HP Network Automation Software

For the Windows®, Linux, and Solaris operating systems

Software Version: 9.21

User Guide

Document Release Date: December 2012
Software Release Date: December 2012

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

© Copyright 2001–2012 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

AMD is a trademark of Advanced Micro Devices, Inc.

Intel and Intel Itanium are trademarks of Intel Corporation in the U.S. and other countries.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Oracle Technology — Notice of Restricted Rights

Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

For the full Oracle license text, after product installation see the `$NA_HOME/server/license` directory (or the `%NA_HOME%\server\license` directory on Windows systems) on the NA application server.

Acknowledgements

This product includes software developed by the Apache Software Foundation. (http://www.apache.org)

Parts of this software Copyright © 2003-2008 Enterprise Distributed Technologies Ltd. All Rights Reserved. (http://www.enterprisedt.com)

Documentation Updates

This guide's title page contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

You can visit the HP Software Support Online web site at:

http://www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software Support Online provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the HP Software Support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Contents

Chapter 1: Getting Started 19
Product Overview 20
    NA 7.50 Features 21
    NA 7.60 Features 22
    NA 9.00 Features 23
    NA 9.10 Features 24
    NA 9.20 Features 25
Help Menu Options 26
NA Home Page 27
Opening a Command Window 28
Accessing Documentation 28
HP Network Automation User Guide 29
    Document Conventions 30
    Send Troubleshooting Page Fields 31
Viewing the Latest Software Version 32
Viewing License Information 32
Viewing System Configuration Pages 33

Chapter 2: Configuring Administrative Settings 35
Getting Started 36
Configuration Management 37
    Configuration Mgmt Page Fields 38
    Change Detection 43
    Syslog Messages 44
    User Attribution Details Page Fields 44
    Configuring Pre-Task and Post-Task Snapshots 45
Device Access 46
    Device Access Page Fields 47
    Per-Task Credentials 52
Server 54
    Server Page Fields 54
Workflow 61
    Workflow Page Fields 61
User Interface 63
    User Interface Page Fields 63
    Customizing the NA Login Page 66
Telnet/SSH 67
    Telnet/SSH Page Fields 67
Reporting 70

    Reporting Page Fields 71
User Authentication 75
    Authentication Failover 75
    LDAP Authentication 76
    SecurID Authentication 76
    TACACS+ Authentication 77
    RADIUS Authentication 77
    HP Server Automation (HP SA) 78
    HP Operations Orchestration (HP OO) 78
    User Authentication Page Fields 79
LDAP External Authentication Setup 82
    LDAP SSL Configuration 83
Server Monitoring 85
    Server Monitoring Page Fields 85
3rd Party Integrations 89
    3rd Party Integrations Page Fields 89
Viewing Monitor Results 91
    System Status Page Fields 91
    Monitor Messages 92
Starting and Stopping Services 96
    Start/Stop Services Page Fields 96
Logging 98
    Log Levels 98
    Log Names 99
    Session Logs 100
    Task Logs 100
    Server Logs 101
    Log Management 101
Troubleshooting Page Fields 102
Reviewing Drivers 103
    Drivers Page Fields 103

Chapter 3: Adding Devices and Device Groups 105
Getting Started 106
    Device Groups Naming Convention 107
Adding Devices 108
    New Device Page Fields 108
    Edit Device Page Fields 113
Bare Metal Provisioning 118
Device Templates 120
    Device Template Page Fields 120
    Device Template Details Page Fields 121
    Edit Template Configuration Page 122
Adding New Device Templates 124
    New Device Template Page Fields 124
    Device Specific Template Page 126
Using the New Device Wizard 127

- New Device Wizard Page Fields 127
Importing Devices 128
- Creating CSV Files for Importing Device Data 128
    - Device Data Import File 129
    - Device Group Data Import File 132
    - Device-Specific Password Data Import File 133
Creating Device Password Rules 134
- Device Password Rules Page Fields 134
- Device Password Rule Page Fields 136
Adding Device Groups 138
- New Group Page Fields 139
Adding Parent Groups 140
- New Parent Group Page Fields 140
- Parent Group Page Fields 141
Dynamic Device Groups 142
- Creating Dynamic Device Groups 142
- Calculating Dynamic Device Groups 143
Device Selector 144
- Selecting Devices 144
- Selecting Device Groups 145
- Device Selector Buttons 145
Viewing Device Groups 146
- Device Groups Page Fields 147
- Device Group Details Page Fields 148
Segmenting Devices and Users 150
Local Realms 152
- Local Realms and NAT Access 152
- Local Realms and Console access 152
- Local Realms and Bastion Host Access 152
- Adding a Local Realm 153
- Overlapping IP Networks 153
- Setting Up The HP Gateway 154
- Gateway List Page Fields 155
- Edit Gateway Page Fields 157
Partitions 158
- Partitions Page Fields 158
- New Partitions Page 159
- Edit Partition Page Fields 159
- Adding Devices to a Partition 160
- Viewing Partition Details 161
Editing Device Groups 162
- Edit Group Page Fields 162
Editing a Batch of Devices 163
- Batch Edit Device Page Fields 163
Discovering Device Drivers 165
Accessing Devices Using Telnet 166

Accessing Devices Using SSH 167

Listing Telnet/SSH Sessions 168

  Telnet/SSH Session List Page Fields 168

  Making Configuration Changes Using The Telnet/SSH Proxy 170

Using a Bastion Host 171

Chapter 4: Managing Device Configurations 173

Getting Started 174

Viewing Device Configuration Changes 174

  Device Configurations Page Fields 175

  Device Configuration Detail Page Fields 177

  Editing Device Configuration Data 180

Comparing Device Configurations 181

  Compare Device Configurations Page Fields 181

Deploying Device Configurations 182

  Deploy Config Task Page Fields 183

Chapter 5: Viewing Devices 187

Viewing Devices 188

  Inventory Page Fields 188

Viewing Device Groups 190

  Device Groups Page Fields 190

Reserving Devices 192

  Activity Calendar 193

Viewing Device Details 195

  Device Details Page Fields 195

NA/SA Integration 198

  NA/SA Permissions 198

  Device Hardware Information 199

  Connecting to NA Through a Firewall 199

  Changing Ports 201

  Incorrect Port Counts 202

View Menu Options 203

  Device Events Page Fields 206

  Device Interfaces Page Fields 207

  Interface Detail Page Fields 208

  Edit Interface Detail Page Fields 210

  Interfaces in Subnet Page Fields 212

  Device IP Addresses Page Fields 213

  Device MAC Addresses Page Fields 214

Virtual Local Area Networks (VLANs) 215

  Device VLANs Page Fields 217

  Creating and Editing VLANs 218

  VLAN Detail Page Fields 219

  VTP Detail Page Fields 220

  VTP Domains Page Fields 221

  VTP Domain Page 222

- Device Blades/Modules Page Fields 222
- Device Policies Page Fields 223
- Servers Page Fields 224
- Device Software Image Recommendation Page Fields 225
- Device Tasks Page Fields 227
- Device Relationships Page Fields 228
- Device Software History Page Fields 230
- Device Sessions Page Fields 231

Edit Menu Options 232
- Device Managed IP Addresses Page Fields 234
- New IP Address Page (Bastion Host) 236
- New IP Address Page (Custom IP Address) 237
- New IP Address Page (Console Server) 238
- New IP Address Page (Hop Box) 239
- New IP Address Page (New Connection Through) 240

Provision Menu Options 241

Connect Menu Options 243

Chapter 6: Managing Users 245

Adding Users 246
- All Users Page Fields 246
- Logged on Users Page Fields 248
- Email Notification 248
- New User Page Fields 249
- Configuring User Passwords 252
  - User Scenario One 252
  - User Scenario Two 253
  - User Scenario Three 253
  - Password Expiration 254
  - Password Reuse 254

Adding User Groups 255
- User Groups Page Fields 255
- New User Group Page Fields 256

Adding User Roles 259
- User Roles & Permissions Page Fields 259
- New User Role Page Fields 261

Editing User Settings 262
- My Settings 262
- My Profile Page Fields 262
- My Workspace Page Fields 264
- My Preference Page Fields 264
- My Permissions Page Fields 266
- Change Password Page Fields 267
- What is Quick Launch? 267
  - How Do I Configure Quick Launches? 268
  - Managing Quick Launches 268
  - Using Quick Launch 269

Sample Quick Launch Display 269
Customizing the NA Home Page 271
My Homepage Tab Fields 272
Statistics Dashboard Tab Fields 274
Search/Connect Function 275

Chapter 7: Scheduling Tasks 277

What Are Tasks? 279
Running Tasks Against Ad-hoc Device Groups 279
Scheduling Tasks 280
Terminology 280
Round-robin Group Tasks 281
Task Templates 282
NA Tasks 284
Configure Syslog Task Page Fields 286
Deploy Passwords Task Page Fields 290
Discover Driver Task Page Fields 295
Reboot Device Task Page Fields 298
Run ICMP Test Task Page Fields 301
Run Command Script Task Page Fields 306
Run Diagnostics Task Page Fields 312
Take Snapshot Task Page Fields 317
Synchronize Startup and Running Task Page Fields 321
Update Device Software Task Page Fields 325
Deployment Table 329
Import Devices Task Page Fields 331
Import Users Task Page Fields 336
Creating CSV Files for Importing User Data 339
Detect Network Devices Task Page Fields 343
Scanning Methods 344
Defining IP Address Ranges 345
Deduplication Task Page Fields 349
OS Analysis Task Page Fields 352
Port Scan Page Fields 355
Provision Device Task Page Fields 358
Add Device Context Task Page Fields 361
VLAN Task Page Fields 365
Configuring Trunk Ports 368
Download Image From Cisco.com Task Page 369
Backup Device Software Task Page Fields 371
Check Policy Compliance Task Page Fields 374
Generate Summary Reports Task Page Fields 377
Email Report Task Page Fields 379
Deploy Remote Agent Page Fields 382
Resolve FQDN Task Page Fields 384
Data Pruning Task Page Fields 387
Run External Application Task Page Fields 390

Scheduling Multi-Task Projects 393
- Sub-task Warning Status 393
- Multi-Task Project Page Fields 395
- How to Configure a Multi-Task Project 397
- Viewing My Tasks 399
- My Tasks Page Fields 399

Viewing Scheduled Tasks 402
- Scheduled Tasks Page Fields 402

Viewing Running Tasks 404
- Running Tasks Page Fields 404

Viewing Recent Tasks 406
- Recent Tasks Page Fields 406
- Task Information Page Fields 408

Viewing Task Load 411
- Task Load Page 411

Chapter 8: Managing Policy Assurance 413

Getting Started 414
- How the NA Policy Manager Works 415

Creating a Policy 416
- Policies Page Fields 417
- New Policy Page Fields 419
- New Rule Page Fields 422

Importing/Exporting Policies 426
- Import/Export Policies Page Fields 426

Editing a Policy 427
- Edit Policy Page Fields 427

Adding a Rule Exception 430
- New Rule Exception Page Fields 430

Viewing Applied Policies 431

Viewing Policy Activity 432
- Policy Activity Page Fields 432

Viewing Policy Compliance 433
- Policy Compliance Page Fields 433
- Configuration Policies That Apply to Device Page Fields 434

Adding New Software Levels 435
- Add Software Level Page Fields 435
- Software Levels Page Fields 437

Editing a Software Level 439
- Edit Software Level Page Fields 439

Testing Policy Compliance 441
- Test Policy Compliance Page Fields 441
- Test Policy Page Fields 441

Chapter 9: Deploying Software 443

Getting Started 444

Software Images 446

Software Images Page Fields 446
Adding Image Sets 447
Add Software Image Set Page Fields 447
Edit Software Image Page Fields 449
Deploying Software 450
Adding a New Software Level 451
Add Software Level Page Fields 451
Viewing Device Software Versions 453
Chapter 10: Event Notification Rules 455
Getting Started 456
Adding Event Rules 461
Event Notification & Response Rules Page Fields 461
New Event Notification & Response Rules Page Fields 462
Event Rule Variables 466
Device Events Variables 466
Variables for Device Configuration Events 467
Variables for Device Diagnostic Events 467
Task Event Variables 468
Variables for All Events 469
Chapter 11: Performing Searches 471
Using the Full-Text Search Functionality 472
Searching for Devices 474
Search For Device Page Fields 475
Device Search Results Page Fields 480
Searching for Interfaces 482
Search For Interface Page Fields 482
Interface Search Results Page Fields 484
Searching for Modules 485
Search For Module Page Fields 485
Module Search Results Page Fields 487
Searching for Policies 488
Search For Polices Page Fields 488
Policies Search Results Page Fields 490
Searching for Policy, Rule, and Compliance 491
Search For Policy, Rule, and Compliance Page Fields 492
Policy, Rule, and Compliance Search Results Page Fields 494
Searching for Configurations 496
Search For Configuration Page Fields 496
Configuration Search Results Page Fields 499
Searching for Diagnostics 500
Search For Diagnostic Page Fields 501
Diagnostic Search Results Page Fields 503
Searching for Tasks 504
Search For Task Page Fields 504
Task Search Results Page Fields 511

Searching for Sessions 513
    Search For Session Page Fields 513
    Session Search Results Page Fields 516
Searching for Events 517
    Search For Events Page Fields 517
    Event Search Results Page Fields 519
    Event Descriptions 520
Searching for Users 525
    Search For Users Page 525
    User Search Results Page 526
Searching for ACLs 527
    Search For ACLs Page Fields 528
    ACL Search Results Page Fields 530
Searching for MAC Addresses 531
    Search For MAC Address Page Fields 532
    MAC Address Search Results Page Fields 534
Searching for IP Addresses 535
    Search For IP Address Page Fields 535
    IP Address Search Results Page Fields 537
Searching for VLANs 538
    Search For VLAN Page Fields 538
    VLAN Search Results Page Fields 540
Searching for Device Templates 541
    Search For Device Template Page Fields 541
    Device Templates Search Results Page Fields 543
SingleSearch 544
    SingleSearch Page Fields 544
    SingleSearch Results Page Fields 546
Advanced Search 547
    Advanced Search Page Fields 547
    Sample Advanced Search 549

Chapter 12: Managing Events and Diagnostics 551
Consolidated View of Events (SingleView) 552
    SingleView Page Fields 553
Diagnostics 555
    Diagnostics Page Fields 555
    New Diagnostic Page Fields 557
Adding & Editing Custom Diagnostics 558

Chapter 13: Custom Data Setup 559
Getting Started 560
    Custom Data Setup Page Fields 560
Enhanced Custom Fields Setup 564
    New Custom Data Field Page 565

Chapter 14: Creating Configuration Templates 567
Getting Started 568

Viewing Configuration Templates 569
    Configuration Templates Page Fields 569
Creating New Configuration Templates 571
    New Configuration Template Page Fields 571
    View Configuration Template Page Fields 573

Chapter 15: Managing Command Scripts 575
Getting Started 576
    HP Operations Orchestration (HP OO) Flows 576
Bare Metal Provisioning Scripts 577
Viewing Command Scripts 579
    Command Scripts Page Fields 579
    Import/Export Scripts/Diagnostics Page Fields 581
Adding Command Scripts 582
    New Command Script Page Fields 584
Creating Auto-remediation Scripts 587
    Auto-remediation Script Syntax 587
    Auto-remediation Script Variable Naming Conventions 588
    Auto-remediation Script Examples 589
Running Command Scripts 596
    Creating a Script from a Configuration Template 596

Chapter 16: Reports 597
Getting Started 598
User & System Reports 599
    User & System Reports Fields 601
Network Status Report 602
    Network Status Report Fields 602
Best Practices Report 605
    Best Practices Report Fields 606
Device Status Report 607
    Device Status Report Fields 607
Statistics Dashboard 608
Diagramming 609
    Diagramming Page Fields 614
    Editing the appserver.rcx file 617
Device Software Report 618
    Device Software Report Fields 618
Software Level Report 620
    Software Level Report Fields 620
Software Vulnerability Report 622
    Software Vulnerability Report Fields 622
Image Synchronization Report 624
    Image Synchronization Report Fields 624
System & Network Events Report 625
    System & Network Events Report Fields 625
    Software Vulnerabilities Event Details Report 626

Summary Reports 627
    Summary Reports Descriptions 628
Emailing Reports 630

Chapter 17: Using SecurID 631

Getting Started 632
Installation Prerequisites 633
    RSA Server Authentication Manager 633
    User Autentication 633
Accessing Network Devices 634
Adding SecurID Software Tokens 636
    New SecurID Tokens Page 636
Logging In Using SecurID 637
    Login Method One: Using a System PIN 638
    Login Method Two: Using a New PIN 638
SecurID Troubleshooting 639

Chapter 18: Compliance Center 641

Getting Started 642
    Compliance Center Home Page 643
COBIT Compliance Status Reports 644
    COBIT Compliance Status Page Fields 645
COSO Compliance Status Reports 652
    COSO Compliance Status Page Fields 652
ITIL Compliance Status Reports 655
    ITIL Compliance Status Page Fields 655
GLBA Compliance Status Reports 658
    GLBA Compliance Status Page Fields 659
HIPAA Compliance Status Reports 661
    HIPAA Compliance Status Page Fields 661
PCI Data Security Standard Compliance Status Reports 668
    PCI Data Security Standard Compliance Status Page 668

Chapter 19: Creating Workflows 669

Getting Started 670
Workflow Wizard 671
My Tasks 673
    My Tasks Page Fields 673
Approval Requests 676
    Approval Requests Page Fields 676
Approving Tasks 678
    Task Information Page Fields 678
Email Notification 681

Chapter 20: Working With ACLs 683

Getting Started 684
Viewing ACLs 685
    Device ACLs Page Fields 685

View ACL Page Fields 687
Running Command Scripts 689
Creating ACLs 690
Changing ACL Applications 691
Batch Inserting ACL Lines 692
Batch Deleting ACL Lines 692
Commenting ACLs and Creating ACL Handles 694
Creating ACL Templates 695
Editing ACLs 696
Deleting ACLs 697
Delete ACLs Task Page 698
Chapter 21: Troubleshooting 701
Driver Discovery Failed 702
Device Snapshot Failed 703
No Real-Time Change Detection Via Syslog 704
Session Logs 705
SWIM Error Messages 706
Appendix A: Command Line Reference 717
Appendix B: Command Permissions 719
Granting Command Permissions 719
List of Commands 720
Command Permission Definitions 721
Appendix C: Sample Scripts 729
Sample PERL Script #1 729
Sample PERL Script #2 730
Sample Expect Script 731
Glossary 733
We appreciate your feedback! 737

Chapter 1: Getting Started

Note: This document is updated as new information becomes available. To check for recent updates, or to verify that you are using the most recent edition of a document, go to:
http://h20230.www2.hp.com/selfsolve/manuals
For more information, see "Documentation Updates" on page 3.

Use the following table to quickly locate information.

Topic	Refer to:
Product Overview	"Product Overview" on page 20
NA 7.50 Features	"NA 7.50 Features" on page 21
NA 7.60 Features	"NA 7.60 Features" on page 22
NA 9.00 Features	"NA 9.00 Features" on page 23
NA 9.10 Features	"NA 9.10 Features" on page 24
NA 9.20 Features	"NA 9.20 Features" on page 25
Menu Bar Options	"Help Menu Options" on page 26
NA Home Page	"NA Home Page" on page 27
Opening a Command Window	"Opening a Command Window" on page 28
Accessing Documentation	"Accessing Documentation" on page 28
Viewing the Latest Software Version	"Viewing the Latest Software Version" on page 32
Viewing License Information	"Viewing License Information" on page 32
Viewing System Configuration Pages	"Viewing System Configuration Pages" on page 33

Product Overview

As networks continue to expand, network topologies continue to increase in complexity. In addition, many networks must now comply with regulations and security best practices. This results in a complex infrastructure with multiple protocols, technologies, and vendors to support.

Centrally managing the network infrastructure in a secure, automated, and centralized fashion becomes vital for the effects of performance — from additional security vulnerabilities to a complete outage — all of which can cause increased liability, lost revenues, and lost productivity.

HP Network Automation (NA) provides an enterprise class solution that tracks and regulates configuration and software changes across routers, switches, firewalls, load balancers, and wireless access points. NA provides visibility into network changes, enabling an IT staff to identify and correct trends that could lead to problems, while mitigating compliance issues, security hazards, and disaster recovery risks. NA also captures full audit trail information about each device change.

Network engineers can use NA to pinpoint the following:

- Which device configuration changed
- What exactly was changed in the configuration
- Who made the change
- Why the change was made

In addition, NA can enforce security and regulatory policies at the network level by making sure that configurations comply with pre-defined standards. The end result is a resilient and maintainable network that is compliant with standards and regulations.

NA supports an array of devices from leading vendors, including HP, Cisco, Nortel, F5 Networks, and Extreme, to provide insights into your network change process. NA's scalable architecture enables you to incorporate the best devices from the best vendors, and support all your devices using one tool.

Note: For information on installing or upgrading NA, see the *NA Installation and Upgrade Guide*.

NA 7.50 Features

NA 7.50 included the following new features:

- Bare Metal Provisioning — Provisions devices out-of-the-box. Using a “bare metal” driver, you can execute scripts against a bare metal device to bring a fully-configured device onto your production network.
- Network Device Templates — Creates a configuration template without having an actual device present. With Network Device templates, you can perform compliance checks, create policy rules, view and compare configurations (even between templates and actual devices), set password rules, and so on before you add the device to the production network.
- Security Partitions — Establishes a set of NA objects per partition to specify more granular permissions. NA objects can include devices, users, command scripts, device password rules, policies, software images, etc. Security Partitions can be combined with a permissions model, group hierarchy, distribution of devices across NA Cores, and network diagramming.
- Auto-Remediation scripts — Defines variables in the script that reference data from regular expression pattern groups in a violated policy rule. The Auto-remediation pop-up window accesses the data on the Policy Rule page to show variable mappings, generate sample code, and validate the script before it is saved. Unlike standard command scripts, Auto-remediation scripts uses a new language syntax to iterate over matches. Auto-remediation scripts are processed and converted into command scripts that are run on network devices.
- NNMi Integration — Integrates NA with NNMi to reside on a single server. As a result, you can:
  - Launch device policy compliance report from NNMi
  - Launch command scripts and diagnostics from NNMi
  - Link to out of the box command scripts and diagnostics with NNMi
  - Designate out of service for devices undergoing change activity
  - Auto-propagate changed community strings to NNMi
  - Auto-config new devices for required NNMi management settings
  - Alert user of duplex and speed mismatch states
- VoIP support — Key elements of VoIP management include:
  - Auto-Detect VoIP, MPLS, PoE and BGP configuration elements within network devices
  - Interface QoS and ACL configuration sections are automatically parsed and displayed in the interface configuration summary for the specific interface
  - A device driver for Cisco Call Manager allowing configuration compliance checks and basic device diagnostics

- Software Image Management (SWIM) process on Gateway server — Displays SWIM-centric data for remote devices. However, remote devices are defined as devices reachable only through an NA gateway.
- HP Operations Orchestration (OO) integration — Enables NA to interoperate with a host of 3rd-party vendors.

NA 7.60 Features

NA 7.60 included the following new features:

- Solaris 64-bit support — When installing NA on a Solaris platform, NA uses the 64-bit Java Virtual Machine (JVM). As a result, NA can utilize more memory.
- Enhanced task scheduling — When creating or updating a task, you can now set a priority for the task so that it runs at higher priority than other tasks. There are five task priority levels, 1 through 5. 1 is the highest task priority level. Higher priority tasks run before lower priority tasks. In addition, you can use the new Round-robin algorithm on group tasks. For example, if you started a group task for 10,000 devices at 10am and then started a group task for 10 devices at 10:05am, using the Round-robin algorithm, you no longer have to wait for the first task group to complete before the second group task is started.
- Enhanced Device Selector and Device Group Explorer — The enhanced Device Selector and Device Group Explorer enable you to easily navigate group trees to select devices and device groups for a variety of applications.
- Multiple VLAN per port support — NA enables you to view and provision VLANs on network switches. With NA, you can:
  - View a complete list of a device’s VLANs
  - View specific VLAN details
  - View a list of ports assigned to a VLAN
  - View trunk ports
  - View a list of VLANs on a trunk port
  - View the native VLAN of a trunk port (the VLAN whose traffic on the trunk port is not tagged)
  - View VTP settings of a network switch
  - Create a new VLAN on a network switch
  - Change a port assigned to a VLAN (add/prune ports)
  - Delete a VLAN
  - Configure a port as a trunk port (multiple VLAN with tagging)
  - Change trunk port VLANs (VLAN membership)
  - Change trunk port native VLANs
  - Configure a trunk port as a non-trunk
- Virtual device and virtual context support — NA now provides support for virtual devices, including VMware's Virtual Switch (vSwitch) technology available via

VMware's Infrastructure (ESX) and the Cisco Nexus 1000V Series switches. These new virtual devices can be managed alongside legacy devices, providing centralized support. Virtual devices, as well as devices which support virtual contexts, including the Cisco Firewall Services Module (FWSM) and Cisco ACE Application Control Engine Module, now benefit from device relationship enhancements that provide management of non-IP address contexts, as well as views of the underlying relationships between the actual hardware and virtual contexts.

- Device relationships — Device relationships maintain data for parent, peer, and child devices. Device dependencies can be defined by the new Device Relationships API.
- Link aggregation support — Link aggregation support enables NA to list all of the links (or connections) associated with a specific port on a device. This information is gleaned from enhanced diagnostics or from new device context information. Link aggregation enables you to manage a device with virtual contexts that assign multiple connections to a physical port.
- Connection Path enhancements — You can now enable or disable device access via primary IP addresses.
- Provisioning and Scripting API enhancements — You can now list device templates, show device template configurations, modify device template configurations, and provision devices using the Device Relationships API.

NA 9.00 Features

NA 9.00 includes the following features:

- Quick Launch — You can now customize tasks and quickly launch them with pre-filled data without having to navigate away from the current page.
- Task Templates — Task Templates enable you to save task definitions so that you can easily configure and run new and existing tasks without having to start from scratch.
- Streamlined Policy Manager — You can now view policies that apply to a device. As a result, you can:
    - Verify that the correct policy was applied to the device
    - View if the policy passed or failed
    - View policies that are applied to the device when the device is added to NA
    - View the exceptions that are in place for a policy applied to the device
- Nmap port scanning — You can now use Nmap for discovering network devices. Nmap can also be used to scan a device's ports and return details on which ports are open and what services they provide. By running the Port Scan task, you can:
    - Easily confirm which ports on a device are open or closed
    - Determine a device's vulnerability based on TCP stack, OS detection, and other Nmap provided services
- Configuration file parsing — For easy navigation, there are now links directly above the configuration text that enable you to quickly parse sections of the configuration file. For example, if the configuration file includes an Access List section, you can click the Access List link at the top of the configuration file and navigate directly to that

section. Note that currently, only the Cisco IOS generic driver supports section parsing.

- SecurID user device authentication — During installation, the NA Installer installs the *rsa_api.properties* file in the *NA_DIRECTORY/jre* directory. You can edit this file to include the IP Address of the server on which NA resides and the location of the RSA conf file that is generated by the RSA Server Authentication Manager.
- FTP server support — NA now has an integrated FTP server and will generally access a device via the CLI to set up data transfer to and from the device.
- Device uptime information — You can now search for a device's uptime and when the Detect Device Boot diagnostic was last run against the device.
- NA user password expiration — The following options are now displayed on the New and Edit User pages for NA system administrators when creating new user profiles or editing existing user profiles:
  - User must change password at next login
  - User cannot change password
  - Password never expires
  - Account is locked out
- NA 9.00 provides a more intuitive user interface, including new main menu drop-down menus for easier navigation and an updated "My Workspace" area.
- Set custom data fields in CLI/API — Previously, several CLI commands had the ability to modify a custom field through the use of the "customname" and "customvalue" options on the command. However, you could only manipulate one field at a time. This was cumbersome if you needed to modify multiple fields. As a result, the new "customnames" and "customvalues" values enable you to specify multiple fields to modify simultaneously.
- New Search and Reporting architecture — The new search and reporting architecture enables NA to more quickly display search results. In addition, new data type fields can be easily added, deleted or modified.
- Improved Logging and Troubleshooting — You can now provide detailed Server logs, Task logs, and Wrapper log information when reporting troubleshooting information.

NA 9.10 Features

NA 9.10 includes the following features:

- Autopass — There are now two types of NA licenses:
  - InstantOn — InstantOn NA licenses are shipped with the product. Each InstantOn license is limited to 250 devices and 60 days of use after installing the product.
  - Permanent — Permanent NA licenses must be obtained via the HP License Key Delivery Service. Permanent NA licenses do not have an expiration date and can be used in conjunction with one NA add-on feature, such as Horizontal Scalability or Multimaster Distributed Systems. For detailed information on NA licenses, see the *NA Installation and Upgrade Guide*.

- Viewing Device Groups — You can now view a listing of devices from the perspective of any of the parent groups in its ancestry. This enables batch editing of devices from the desired parent group's perspective. In addition, there is now a tree presentation of the Device Groups page. This replaces the previous multi-page, drill-down navigation design.
- Email Notification — You can now send and receive emails from logged-on NA users.
- Policy Manager API — You can now create policies using the NA API. There are now CLI commands for creating policies, creating rules within policies, creating remediation scripts for the rules, modifying existing policies, and so on. For information, see the *NA CLI/API Command Reference*.
- NNMi-NA Integration — The NNMi-NA Integration Connector is no longer used in NA. NNMi-NA integration occurs via the WebServices call between the two products. The new NNMi-NA integration:
  - Simplifies deployment
  - Improves topology synchronization reliability
  - Increases synchronization speed between NNMi and NA
  - Supports single sign-on between NA and NNMi (you can move between the two product consoles without logging on again)

  To enable the HP NNMi–HP NA integration, follow the procedure in the *HP Network Node Manager i Software—HP Network Automation Integration Guide*.
- SNMP v3 Support — Network devices using SNMPv3 for device discovery are now detectable. Using less secure network device detection methods is avoided when SNMPv3 protocol is used, enabling the use of the most up-to-date SNMP security mechanisms.

NA 9.20 Features

NA 9.20 includes the following features:

- HP NNMi–HP NA Integration improvements:
  - The integration now supports SSL connections between NA and NNMi.
  - The NNMi nodes, interfaces, and incidents forms include new tabs containing NA data (current device configuration, configuration history, and interface configuration) in the analysis pane.

  For information on the HP NNMi–HP NA integration, see the *HP Network Node Manager i Software—HP Network Automation Integration Guide*.
- Import user data — You can now import user and user group definitions from CSV files.
- Import device data improvements — You can now import custom attributes for devices and device groups from CSV files.
- Task completion notification — You can now configure tasks to send email messages upon completion.
- Support for Oracle RAC.

- Improved searching:
  - Case-insensitive search for most fields with Oracle databases. (Microsoft® SQL Server and MySQL database searches are case-insensitive by default.)
  - Faster search for device configurations using the “contains (full text)” operator.
- Improved database pruning gradually reduces the size of the NA database.
- Updated PCI (formerly Visa CISP) compliance report.
- Performance improvements, including reduced data storage
- New deployment architecture for disaster recovery using Oracle GoldenGate. For information, see the *NA Disaster Recovery Configuration Guide*.
- Driver improvements:
  - Support for additional virtual devices
  - Additional IPv6 support
  - PERL API support for JavaScript drivers
  - SFTP client support
  - Ability to enforce the saving of configurations on a per-task basis
  - Support for directory structures for the filesystem diagnostic and Software Center
  - DSD_Feature_Index.html, a list of all drivers with each driver's feature matrix and a link to each driver's individual DSD
  - DSD_SYSOID_Mapping_Index.html, a master list of all supported / tested sysOIDs by driver package / driver name / driver description

Help Menu Options

The following options are available from the Help drop-down menu:

- Documentation — Opens the HP Network Automation Documentation page. Note that context-sensitive online Help information is available from the Help link on each NA page.
- Support — Opens the HP Customer Support page. This site provides HP customers with the most recent patch releases and documentation. In addition, you can upload files for issue resolution and troubleshooting.
- HP Live Network — Opens the HP Live Network page, where you can download Security Alert Service data and other NA Content Service material. HP Live Network is a complementary content delivery service that is integrated into HP Network Automation and can deliver periodic network security and compliance content updates.

In addition, the HP Live Network portal hosts:

  - Driver packs
  - The specialized NDS driver development forum
  - The general NA community forum

  The HP Live Network security and compliance service enables immediate assessment of network security and policy violations, as well as automated remediation options. HP Live Network includes valuable free content as well as subscription services. Refer to "Software Vulnerability Report" on page 622 for information.

  Note: For information on installing the HP Live Network Service, see the *NA Installation and Upgrade Guide*.

- About HP Network Automation — Opens the About HP Network Automation page, where you can view information about HP Network Automation. Refer to "Viewing the Latest Software Version" on page 32 for detailed information on the About HP Network Automation page.

NA Home Page

The NA Home page opens whenever you login to NA. You can also return to the NA Home page by clicking the Home link in the upper left-hand corner of each page.

The NA Home Page includes two frames. The left-hand frame includes:

- Search — The Search options enable you to find devices by Hostname or IP address and connect to them via Telnet or SSH. Refer to "Search/Connect Function" on page 275 for detailed information.
- My Workspace — The My Workspace area includes the following sections:
  - Current Device/Current Device Group (Inventory is the default)
  - My Favorites
  - Quick Launches
  - My Settings

Refer to "Editing User Settings" on page 262 for detailed information on configuring the options in the My Workspace area.

The right-hand frame can be customized to include a snapshot of recent configuration changes in the past 24 hours, various system events, and tasks requiring your approval. Refer to "Customizing the NA Home Page" on page 271 for information.

Opening a Command Window

To open a command window, in the Search tab on the left-hand side of the display, enter a device IP address or hostname and click the Connect button. You can also open a command window from the Device Details page using the Connect menu. Within the command window, you can select the text that you want to copy and press the Return key. The highlighted text is placed into a copy buffer. You can then paste it into another application. Enter `exit` and close the window when you are finished.

Note: If you use the Telnet/SSH Proxy to connect directly to devices, you remain in the Telnet/SSH Proxy when you exit the device. Unless you enter `exit` again, you can enter CLI commands and connect to other devices.

To view Help for CLI commands, enter: `help` to see a list of all commands. Enter `help <command name>` to see detailed help on a specific command.

Accessing Documentation

The core NA Documentation Set includes:

- *NA User Guide*— To view the PDF version, after logging in, from the Help drop-down menu, click Documentation. The HP Network Automation Documentation page opens. Select *HP Network Automation User Guide* from the list.
- NA Help Files — To view the online Help files, after logging in, click the Help link at the top of any NA page.
- *NA Installation and Upgrade Guide* — To view the PDF version, after logging in, from the Help drop-down menu, click Documentation. The HP Network Automation Documentation page opens. Select *HP Network Automation Installation and Upgrade Guide* from the list.
- *NA Release Notes* — To view the PDF version, after logging in, from the Help drop-down menu, click Documentation. The HP Network Automation Documentation page opens. Select *HP Network Automation Release Notes* from the list.

If you are interested in additional NA publications, including the documentation listed below, please navigate to the NA Support site:

- *NA Multimaster Distributed System on Oracle Guide*
- *NA Multimaster Distributed System on SQL Server Guide*
- *NA Horizontal Scalability Guide*
- *NA Satellite Guide*

HP Network Automation User Guide

This guide includes information on:

- Setting up and configuring the system
- Adding and configuring devices and device groups
- Adding users, groups, and roles
- Creating Workflows
- Using SecurID, TACACS+, and RADIUS to access network devices
- Importing users and user groups from LDAP
- Managing Access Control Lists (ACLs)
- Using the Compliance Center
- Searching for information, creating custom reports, and running summary reports
- Deploying configurations
- Viewing and provisioning VLANs
- Configuring device relationships
- Creating event rules and event notifications
- Viewing default diagnostics
- Creating and running diagnostics and command scripts
- Creating company-wide policy rules to prevent inconsistency
- Deploying device software from a central repository
- Connecting to devices using Telnet and SSH
- Running the command line interface (CLI)
- Exchanging data with other IT applications using Java and PERL APIs
- Using online Help, contacting Customer Support, and updating your software license

Note: The *NA User Guide* provides information on all options available to the NA System Administrator. Depending on your permissions, some of the NA menu options could be grayed-out.

Document Conventions

The following table explains the conventions used in this guide.

Convention	Description/Action
Italic	Used for system messages, paths, file names, and Web URLs. For example, *C:\hp\sdk\docs*.
Link	Moves you from one location to another within a document, opens Web pages, or opens a new email message. Cross-references within this guide are contained within quotation marks and include a page number, while links to URLs and email addresses appear as underlined text.
Enter	Indicates that you should type the text or command that follows, then press the Enter key on the keyboard.
< >	Indicates variable information, such as a name or folder that you must supply. Do not include the angle brackets when replacing the placeholder.

Send Troubleshooting Page Fields

To send troubleshooting information to Customer Support:

1. On the menu bar under Admin, click Troubleshooting. The Troubleshooting page opens.
2. Click the Send Troubleshooting Information link at the top of the page. The Send Troubleshooting Info page opens.

Note: You must have Administrative privileges to be able access logs files.

Fields	Description/Action
To	Enter your email address if it is not already displayed.
Subject	The subject line, "HP Network Automation Info," is displayed.
Problem Number	Enter the problem number related to an open ticket, if applicable.
Comments	Enter comments regarding the issue. Be sure to include your return email address and direct phone (or cell number). The contact information on file is not always accurate or specific to the person with the issue.
Include	Select one or more of the following options: • Server logs for the last < > hours — Enter the number of hours worth of stored logs you want to send. The default is 4. • Administrative settings — Include the collection of Administrative settings and options in effect for your NA server. • System Status File — A file created to provide system status information. • Wrapper Log — If requested, this sends the Jboss_Wrapper log file. • Task Logs — A list of available task log files. Each file lists the task type, task ID, device (if applicable), and time the task completed.

Be sure to click Send when finished.

Note: The Download Troubleshooting Info page enables you to download troubleshooting information. The page is identical to the Send Troubleshooting page, except that there are no To, Subject, Problem Number, or Comments fields. In addition, the Send button reads Download.

Viewing the Latest Software Version

To view the About HP Network Automation page, from the Help drop-down menu, click About HP Network Automation. The About HP Network Automation page opens.

You can view detailed information about the current NA software version. In addition, this page includes the following links:

- Download Driver Update Packages — Displays the HP BSA Essentials Network web site.
- View Latest Release Notes — Displays the HP Passport sign-in page.
- View License Information — Refer to "Viewing License Information" on page 32 for information.
- Contact Customer Support — Displays the Software Support Online web site.
- View System Configuration — Refer to "Viewing System Configuration Pages" on page 33 for information.

There is also a list of device drivers installed on your system. Refer to the Driver Release Service (DRS) documentation for detailed information on supported devices. The DRS is an automated driver release and delivery system.

Viewing License Information

The License Information page enables you to determine:

- To whom your product is licensed.
- How many nodes the license includes.
- How many nodes are in use.
- When your license expires.

You can also update your license from this page.

To view the License Information page:

1. From the Help drop-down menu, click About HP Network Automation. The About HP Network Automation page opens.
2. Click the View License Information link. The License Information page opens.

Fields	Description/Action
Product	Displays the software version you are licensed to use.
Licensed to	Displays the name of your company or division.
Number of nodes licensed	Displays the number of nodes the software is allowed to recognize. Keep in mind that some devices, such as the Cisco 6500, contain cards that operate as separate nodes.
Number of nodes in use	Displays the number of nodes activated in NA.
License expiration	Displays when your software license expires.
Update License button	When it is time to update your software license, HP sends you new license text. Paste the text into the box, then click Update License to install the new license.

Viewing System Configuration Pages

If the Distributed System is enabled and you have configured NA Cores, the View System Configuration page enables you to determine:

- How many NA Cores are configured
- How many Partitions are configured

Refer to "Segmenting Devices and Users" on page 150 for information on Overlapping IP Networks and Restricted Device and User Views. For information on installing and configuring a Multimaster Distributed System, see the *NA Multimaster Distributed System on Oracle Guide* or the *NA Multimaster Distributed System on SQL Server Guide*.

Chapter 2: Configuring Administrative Settings

Use the following table to quickly locate information.

Topic	Refer to:
Getting Started	"Getting Started" on page 36
Configuration Management	"Configuration Management" on page 37
Device Access	"Device Access Page Fields" on page 47
Server	"Server" on page 54
Workflow	"Workflow" on page 61
User Interface	"User Interface" on page 63
Telnet/SSH	"Telnet/SSH" on page 67
Reporting	"Reporting" on page 70
User Authentication	"User Authentication" on page 75
LDAP Authentication Setup	"LDAP External Authentication Setup" on page 82
Server Monitoring	"Server Monitoring" on page 85
3rd Party Integrations	"3rd Party Integrations" on page 89
Viewing Monitor Results	"Viewing Monitor Results" on page 91
Starting and Stopping Services	"Starting and Stopping Services" on page 96
Logging	"Logging" on page 98
Reviewing Drivers	"Reviewing Drivers" on page 103

Getting Started

As the System Administrator, you can define values for configurable settings that affect HP Network Automation (NA) operation. These settings receive initial values during installation, but you can change the values to customize features. For example, you can change the default values for intervals associated with various operations, or configure support for scripting languages. You can also customize the appearance and content of certain pages.

To review the configuration options and make changes, on the menu bar under Admin, select Administrative Settings. You can select the following options:

- Configuration Management
- Device Access
- Server
- Workflow
- User Interface
- Telent/SSH
- Reporting
- User Authentication
- Server Monitoring
- 3rd Party Integrations

Configuration Management

The Configuration Mgmt page enables you to configure:

- Configuration change detection
- User identification
- Startup and running configurations
- ACL parsing and editing
- Configuration policy verification
- Pre-task and post-task snapshots
- Diagnostics
- Flash storage space
- Boot Detection
- Custom Service Types

To view the Configuration Mgmt page, on the menu bar under Admin select Administrative Settings and click Configuration Mgmt. The Configuration Mgmt page opens. Be sure to click Save to save your changes.

Configuration Mgmt Page Fields

Field	Description/Action
Change Detection	
Change Detection	Select one of the following options: • Enabled — NA takes device configuration snapshots whenever changes are detected (the default). • Polling Only — NA takes device configuration snapshots during device group snapshots, but not when changes are detected. • Disabled — Configuration snapshots are not taken in response to detected changes or during device group snapshots. Refer to “Change Detection” on page 43 for detailed information on change detection.
Change Detection Interval	Enter the delay interval between detection of a change and the snapshot. The default is 10 minutes. When NA detects a change, the device snapshot is delayed for the interval specified here. The subsequent snapshot reflects all change notifications sent during the interval.
Syslog Detection Patterns	If you want to add a pattern to the default patterns supplied by NA, enter a pattern in the right-hand box and click Add Pattern <<. You can select a pattern from the left-hand box and click Delete Pattern to delete a pattern. NA looks in the Syslog server for matches to these patterns. When NA finds a match, it indicates a configuration change and takes a snapshot of the device configuration, if enabled above. (**Note**: HP provides a Syslog server. If you kept your current Syslog server when you installed NA, you still must install the NA Syslog server and relay Syslog messages to the NA Syslog server.) Refer to “Syslog Messages” on page 44 for detailed information on Syslog message patterns.
Syslog Patterns to Ignore	If you want to ignore a pattern, enter a pattern in the right-hand box and click Add Pattern <<. You can select a pattern from the left-hand box and click Delete Pattern to delete a pattern.
Secondary IP Types	Select a Secondary IP type. Primary and Alternate are selected by default. Secondary IP types are used for change detection Syslog event handling for secondary IP addresses. Note that not all secondary IP addresses are included in Syslog event handling. You can select from the following options: • Primary • Alternate • Console • Hop Box • NAT • Connect Through • Internal Through • Internal Direct Refer to “Device Managed IP Addresses Page Fields” on page 234 for information on managing IP addresses.

Field	Description/Action
Use IP Address of sender of Syslog Messages	If checked, the IP address of the Syslog messages sender is used.
Users to Ignore for Change Detection	Indicate the users to ignore when processing Syslog or AAA change events. To add a user, enter the user name in the right-hand box and click Add Username <<. To delete a user select the username in the left-hand box and click Delete Username.
Change User Identification	
Auto-Create Users	If checked, NA creates a new user if it does not recognize the author of a configuration change.
Auto-Create User Suffix	Enter the suffix that NA appends to new users per the Auto-Create feature. The default is "_auto".
Syslog User Identification	If checked, NA tries to identify users from Syslog messages.
Syslog User Patterns	The Syslog User Patterns are Java regular expressions. You add a capturing group to indicate where the username is in the regular expression, for example: • User (\S+) authenticated • session opened for user (\S+) • Login successful for user (\S+) on NA uses these patterns to determine which user is responsible for a configuration change. Enter a pattern in the right-hand box and click Add Pattern <<. You can select a pattern in the left-hand box and then click Delete Pattern to delete the pattern. NA looks in the Syslog for matches to these regular expressions. When NA finds a match, it captures the text as a user. Normally, the device drivers populate these patterns.
Resolve Workstation IP Address from Syslog	If checked, NA resolves the IP address from the Syslog message and treats the domain name as the username responsible for the related configuration change. This method is used only if the username cannot be determined in other ways from the Syslog message.
Store Unresolved IP Addresses	If checked, when a host name using DNS cannot be resolved, NA treats the IP address as a username. Periods are replaced by dashes. For example, 10.10.1.1 becomes user 10-10-1-1.
Auto-Create Users from Syslog	If this option and Auto-Create Users are checked, NA attempts to match users identified from Syslog messages to existing users. When there is no existing user, a new user is created.

Field	Description/Action
Startup/Running Configurations	
Capture Startup Config	Select one of the following options: • Off — NA does not capture each startup configuration. • Detect Only — NA captures each startup configuration and compares it to the running configuration, but does not store the startup configuration. • On (the default) — NA captures each startup configuration, compares it to the running configuration, and stores the startup configuration. Keep in mind that not all vendors and devices support the concept of a startup configuration.
ACL Parsing	
Parse ACL Data with each Snapshot	Select one of the following options: • Enabled — NA parses and stores ACL data with each snapshot. • Disabled — NA does not parse ACL data with each snapshot. Keep in mind that this option only sets the default state of this feature when adding new devices. You can use batch editing to turn on and off ACL parsing for groups of devices. (**Note**: This option can be overridden on a device-by-device basis.)
ACL Editing	
Show pre-edit application script	If checked, the script for pre-processing ACL applications is displayed when editing or creating ACLs. The pre-application script negates the existing applications of an ACL on the device. The new or updated ACL script adds the edited ACL to the device.
Show edit preparation script	If checked, the edit preparation script is displayed when editing or creating ACLs. The edit preparation script performs any necessary scripting to prepare the device to accept the edited ACL.
Show application script	If checked, the ACL application script is displayed when editing or creating ACLs. The application script is the piece of scripting used to apply an ACL, for example to a VTY connection. The application script re-applies the ACL.
Configuration Policy Verification	
Verify Before Deploy by Default	If checked, NA checks edited configurations against defined configuration policies before deployment.
Pattern Timeout	Enter the maximum number of seconds a pattern can take to match a configuration. The default is 30 seconds.
Run Auto-remediation Script	If checked, controls whether auto-remediation scripts should be allowed to run automatically after a rule is found non-compliant. Refer to "Creating Auto-remediation Scripts" on page 587 for information on auto-remediation scripts.
Automatically apply imported policies to the Inventory group	If checked, all imported policies are applied to the Inventory group.

Field	Description/Action
Pre-Task and Post-Task Snapshots	
User Override Pre/ Post Task Snapshot	If checked, enables users to override the default pre-task and post-task snapshot settings when running individual tasks. If override is allowed, the pre and post task snapshot options are displayed on New Task pages, where applicable. If override is not allowed, the default setting is used. (Refer to "Configuring Pre-Task and Post-Task Snapshots" on page 45 for detailed information.)
Allow Per-Script Pre/ Post Task Snapshot Setting Hints	If checked, enables individual scripts to override pre-task and post-task snapshot settings. **Note**: To override the pre-task snapshot setting, include a comment in the script with the text "tc_pre_snapshot=true" to request a pre-task snapshot or "tc_pre_snapshot=false" to request no pre-task snapshot. To override the post-task snapshot setting, include a comment in the script with the text "tc_post_snapshot=true" to request a post-task snapshot as part of the task, "tc_post_snapshot=task" to request a post-task snapshot as a separate task, or "tc_post_snapshot=false" to request no post-task snapshot. Refer to "Configuring Pre-Task and Post-Task Snapshots" on page 45 for detailed information.
Snapshot Before Run Command Script	Select one of the following options: • None (default) • As part of task
Snapshot After Run Command Script	Select one of the following options: • None • As part of task (default) • Scheduled as separate task
Snapshot Before Configuration Deployment	Select one of the following options: • None • As part of task (default)
Snapshot After Configuration Deployment	Select one of the following options: • None • As part of task (default) • Scheduled as separate task
Snapshot After Provisioning Device	Select one of the following options: • None • As part of task (default) • Scheduled as separate task
Snapshot Before Run Diagnostic	Select one of the following options: • None (default) • As part of task

Field	Description/Action
Snapshot After Run Diagnostic	Select one of the following options: • None (default) • As part of task • Scheduled as separate task
Snapshot Before Delete ACL	Select one of the following options: • None • As part of task (default)
Snapshot After Delete ACL	Select one of the following options: • None • As part of task (default) • Scheduled as separate task
Snapshot After Synchronize Startup/ Running	Select one of the following options: • None (default) • As part of task • Scheduled as separate task
Post-Task Snapshot Delay	Enter the delay for any post-task snapshots that run as separate snapshot tasks (if any). The default is 30 seconds.
Diagnostics	
Topology Data Gathering Frequency	Topology data is included in a new class of diagnostics that requires throttling to preserve network performance. Topology data is used to render network diagrams. Gathering topology data represents a significant load on the NA server and should be done as infrequently as possible. Enter the minimum amount of time (in hours) allowed between attempts to gather topology data. The default is 168 hours.
Stored Topology Data	Enter the allowable age (in hours) of topology data currently stored in the database. If the stored data is older than this value, data will be retrieved directly from the device. Otherwise the stored data will be used. The default is 72 hours.
Duplex Data Gathering Frequency	Duplex mismatch data is included in a new class of diagnostics that requires throttling to preserve network performance. Duplex mismatch data is used to identify a common end-to-end performance problems. Often times a duplex mismatch occurs when one machine is set at full-duplex and another at half-duplex. Gathering duplex mismatch data represents a significant load on the NA server and should be done as infrequently as possible. Enter the minimum amount of time (in hours) allowed between attempts to gather duplex data. The default is 168 hours.
Stored Duplex Data	Enter the allowable age (in hours) of duplex data currently stored in the database. If the stored data is older than this value, data will be retrieved directly from the device. Otherwise the stored data will be used. The default is 72 hours.
Flash Storage Space	
Flash Low Event	If checked, an event is generated if the detected available flash storage space is low.
Flash Low Threshold	Enter the percentage of flash storage space that must be filled before a low space event is generated. The default is 90%.

Field	Description/Action
Boot Detection	
Error Margin Factor	Enter how much clock drift (in seconds per six hours) to allow for when detecting device boots. It is recommended that the minimum frequency with which you check your devices be once every six hours.
Custom Service Types	
Custom Service Types	Add or delete a Service Type. Service Types can specify VoIP, BGP, MPLS, and so on for a device. The values help to identify the device's purpose. Refer to "Viewing Device Details" on page 195 for more information on Service Types.

Change Detection

NA uses several methods for detecting changes to a device configuration, including:

- Syslog messages
- AAA log reading
- Internal proxy

From these methods, NA uses a number of different inputs to determine who actually made a change on the device. This information provides the most likely user responsible for the change. In order of priority, the following information is used:

- User who scheduled a password change that was run on the device.
- User who scheduled a software update that was run on the device.
- User who deployed a configuration to the device.
- User who ran a script on the device.
- User who connected to the device via NA's proxy.
- User information gathered from AAA logs.
- User information parsed out of a syslog message.

NA assigns a change attribution to a device interaction that is higher in the priority list. For example, if a user schedules a password change while another user had proxied to the device during the same time period, if a change had been detected, that change would be assigned to the user who had scheduled the password change.

To view configuration changes on a device:

1. On the menu bar under Devices, click Inventory. A list of all currently managed devices opens.
2. Click the device for which you want to view configuration changes. The Device Details page opens.
3. From the View drop-down menu, click Configuration Changes.
4. In the Changed By column, click the Details link. The User Attribution Details page opens.

Syslog Messages

The NA Core Syslog server forwards Syslog messages to the NA Core that match a list of Syslog patterns for the drivers that are in-use on the system. When the Discover Driver task runs, it updates the list of Syslog message patterns to look for, and then instructs the NA Syslog server to update its list of Syslog message patterns.

The NA Satellite Syslog server does the same thing. It includes a list of Syslog message patterns for in-use devices and only forwards messages to the NA Core that match one of those patterns. As a result, when you run the Deploy Remote Agent task, the following message is displayed: `Initialized Satellite with N syslog change detection patterns from Core.`

The initial NA Satellite receives the current Syslog message pattern list. Subsequent Discover Driver tasks notify both the NA Core Syslog server and the NA Satellite Syslog servers when new devices are discovered that require new Syslog patterns.

User Attribution Details Page Fields

Note: Not all configuration changes can be attributed to a “user” and could be marked as N/A.

Field	Description/Action
Change Event Detail	
User	Displays the name of the user who made the change.
Date	Displays the date the change was made.
Device Interaction	Displays the method used to detect the change, for example Syslog.
Additional Details	Displays additional details about the change, for example if the change was made from the console.

Configuring Pre-Task and Post-Task Snapshots

Configuring pre-task and post-task snapshots enables you to:

- Define the pre and post snapshot behavior for various task types
- Run post snapshots as separate tasks
- Override the default pre-task and post-task snapshot behavior when running a specific task

Pre-task and post-task snapshot options can be displayed for the following tasks:

- Deploy Config (refer to "Deploy Config Task Page Fields" on page 183)
- Run Diagnostics (refer to "Run Diagnostics Task Page Fields" on page 312)
- Delete ACL (refer to "Delete ACLs Task Page" on page 698)
- Synchronized Startup and Running (refer to "Synchronize Startup and Running Task Page Fields" on page 321)
- Run Command Script (refer to "Run Command Script Task Page Fields" on page 306)
- Batch Insert ACL Line (refer to "Batch Inserting ACL Lines" on page 692)
- Batch Remove ACL Line (refer to "Batch Deleting ACL Lines" on page 692)

When providing snapshot hints in command scripts, you can add a special tag to a command script to specify the pre or post task snapshot behavior when running that script. For example, suppose you have an advanced script that does not actually connect to or modify a device. The advanced script simply uses the NA API to extract information about a device and generate a report. In that case, there is no need to take a snapshot after the task is run, so the advanced script could include a tag to indicate that no post snapshot is needed.

Keep in mind that if more than one script is selected to run against a group of devices, and more than one of the scripts contains a hint, the most conservative behavior among those specified is used.

Device Access

The Device Access page enables you to:

- Designate device connections methods
- Configure Detect Network Devices task settings
- Configure Bastion host settings
- Configure SecurID device access
- Configure SSH device access
- Specify what credentials should be used to access devices on a per-task basis
- Designate Nortel BayRS MIB/OS versions
- Enter Gateway Mesh information

Network environments are often protected by network firewalls. NA provides four methods for accessing devices through firewalls:

- Open up direct access through the firewall.
- Create a Network Address Translation (NAT) on the firewall and configure NA to use the NAT to access the device. Keep in mind that NAT addresses do not appear on the device configuration for the device using the NAT.
- Configure NA to use an existing bastion host on the far side of the firewall to proxy management requests. Since bastion hosts are already allowed access through the firewall, the bastion host configuration enables management of a device through a proxy connectivity of the bastion host.
- Using a Gateway Mesh. (For information, see the *NA Satellite Guide*.)

Keep in mind that a console server maintains a physical connection to the device using the serial link. These links are provided through Telnet to specific IP port numbers hosted on the console server. Console server connections are available even if the network device is disconnected from the network.

To view the Device Access page, on the menu bar under Admin select Administrative Settings and click Device Access. The Device Access page opens.

Device Access Page Fields

Field	Description/Action
Device Connection Methods	
Password Selection	Select one of the following options: • Always try last successful passwords first. — If checked, NA first tries the last successful password from the previous access to the device. If the last successful password changes in the middle of the task, the new last successful password is not guaranteed to be used for the remainder of that task. In addition, the "Last used rule changed" event will continue to be generated. Consequently, you can determine when devices are not using their expected password rule. • Always try passwords in defined order. — If checked, NA always tries passwords in a defined order. Keep in mind that NA keeps track of the most recently used authentication credentials for the next round of communications with a device. This enables you to take advantage of the Device Password Rules, while minimizing the number of connection attempts to each device. Refer to "Creating Device Password Rules" on page 134 for more information.
Default Connection Methods	The following methods are used to connect to devices. These methods appear checked by default on the New Device page and in the Add Device wizard. Check one or more of the following options: • Telnet • SSH • RLogin • SNMP • SCP • FTP • TFTP **Note**: NA has an integrated TFTP server and will generally access a device via SNMP or CLI to set up the transfer to and from this device. For devices that have their own TFTP server, NA acts as a TFTP client. Typically, SCP must be used with the CLI. SCP requires a device be enabled to use SSH. SCP cannot run if the device does not have a SSH server running. NA also provides an integrated FTP server and will generally access a device via the CLI to set up the transfer to and from the device.
Bad Login Attempt Delay	Enter the number of seconds to delay after a bad login attempt to allow the device time to recover. The default is five seconds.
SNMP Timeout	Enter the number of seconds to delay while waiting for a device to operate on a set of SNMP commands (such as loading a config). The default is 40 seconds.
Maximum number of Password Attempts	Enter the maximum number of password attempts allowed. Zero (0) represents no limit. Keep in mind that if you have 10 password rules and you enter 3, NA stops after the first three password rules are tried. This setting is useful if your TACACS server locks out usernames after three failed login attempts. You can enter 1 if you want to try only one password rule. This setting is useful if only one password rule works.
Maximum Archived Rules	Enter the maximum number of archived password rules to try. The default is 3. To disable this option, enter 0.

Field	Description/Action
Detect Network Devices Task Settings and Port Scan Task Settings	
Path to Nmap utility	Enter the path to the Nmap utility for scanning network devices. (**Note**: Nmap enables you to scan networks to determine which ports are up and the services they offer. Refer to www.Insecure.Org for detailed Nmap information.) For information on installing Nmap, see the *NA Installation and Upgrade Guide*.
Allow Nmap Port Scan	If checked, users with the appropriate permissions can use Nmap to scan network devices. Refer to "Port Scan Page Fields" on page 355 for information on using Nmap.
Nmap Port Scan Option	Displays the default option when using Nmap to scan network devices. Nmap controls how a device scan is performed. As the default, NA passes -PO to Nmap telling Nmap to work over IP instead of UDP. Refer to the Nmap documentation for a complete list of options. Refer to "Port Scan Page Fields" on page 355 for additional information on using Nmap.
Max Addresses to Discover Per Task	Enter the maximum number of IP addresses to discover. Be sure to limit Detect Network Devices tasks to the maximum number of addresses (1024 is the default) to scan to reduce network traffic.
Max SNMP Scanner Threads	Enter the maximum number of SNMP scanner threads the Detect Network Devices tasks will spawn during device discovery using the SNMP scanning method. The default is 79. Theoretically, the higher the maximum SNMP scanner thread count, the faster the task runs. However, having too many SNMP scanner threads can impact system performance due to CPU overhead and network traffic that each SNMP scanner thread requires. (**Note**: When configuring the Detect Network Devices task, you have the option to have the Detect Network Devices task use SNMP to detect devices. As a result, the task will spawn many SNMP scanner threads that communicate to devices via SNMP. Refer to "Detect Network Devices Task Page Fields" on page 343 for information on other scanning methods.)
Network Discovery IP or CIDR Range Exclusions	Enter IP addresses or Classless Inter-Domain Routing (CIDR) range exclusions (for example: 192.168.1.0-192.168.2.0 or 192.168.31.0/24) in the right-hand box and click the Add Pattern << button. Ranges are inclusive. To delete patterns, select the patterns from the left-hand box and click the Delete Pattern button.
SNMP Timeout	Enter an SNMP timeout value in milliseconds for each SNMP SysOID probe. The default is 500ms.
Bastion Host Settings	
Use Bastion Host by Default	If checked, new devices use bastion host for Telnet and SSH access. (**Note**: Bastion Host settings can be overridden on a device-by-device basis.)
Default Bastion Host	Enter the hostname or IP address of the bastion host to use for Telnet and/or SSH access.
Default Bastion Host Username	Enter the username of the bastion host to use for Telnet and/or SSH access.
Default Bastion Host Password	Enter the password of the bastion host to use for Telnet and/or SSH access.

Field	Description/Action
SecurID Device Access	
SecurID License Usage	Select one of the following options: • Use Unique Tokens Per User — If checked (the default), each device access will use only the seed(s) corresponding to the user that initiated the task or Telnet/SSH proxy connection. • Use Software Token Pool — If checked, a pool of general use software token seeds are provided and used as efficiently as possible for maximum performance. Enter the username for which the pool of SecurID Software Tokens are associated. Using unique Software Tokens per user requires more tokens, and increases token maintenance. Using Software Tokens from a pool with a common user reduces the number of tokens required, and potentially increases task throughput.
Max Software Tokens	Enter the maximum number of Software Token licenses imported to the machine running NA. The default is 1024.
Passcode Lifetime	Enter the lifetime for Software Token passcodes. The default is 60 seconds.
FTP and SSH Device Access	
FTP/SSH User	Enter a FTP or SSH user. The FTP or SSH username is used when accessing the FTP or SSH server via a device connection. If this username does not exist in the system FTP or SSH server, it will be created automatically. **Note**: When using SCP on a Linux or Solaris platform, you will need to modify your system's SSH daemon (SSHD) to run on an alternate port and restart the SSHD service. Port 8022 is recommended. Keep in mind that the device specific settings must be configured to enable SCP and SSH to function properly. In addition, the device and the device driver must support SCP to use the NA SSH server for SCP.
FTP/SSH Password	Enter a FTP or SSH password. The FTP or SSH password is used when accessing the FTP or SSH server via a device connection.

Field	Description/Action
Task Credentials	
Allow Standard Device Credentials	Select one or more of the following tasks. By default, all of the tasks are selected. • Configure Syslog • Delete ACLs • Deploy Configuration File • Deploy Passwords • Discover Driver • Reboot Device • Run Command Script • Run Diagnostics • Run ICMP Test • Synchronize Startup and Running • Take Snapshot • Update Device Software The above tasks enable users to select standard processing with device-specific passwords and/or network-wide password rules. For information on per-task credentials, refer to "Per-Task Credentials" on page 52. For information on password rules, refer to "Device Password Rule Page Fields" on page 136.
Allow Per-Task Device Credentials	Select one or more of the following tasks. • Configure Syslog • Delete ACLs • Deploy Configuration File • Discover Driver • Deploy Passwords • Reboot Device • Run Command Script • Run Diagnostics • Run ICMP Test • Synchronize Startup and Running • Take Snapshot • Update Device Software If checked, the above tasks will prompt users to enter one-time use device credentials specific to that task. For information on per-task credentials, refer to "Per-Task Credentials" on page 52.

Field	Description/Action
Allow User AAA Credentials	Select one or more of the following tasks. • Configure Syslog • Delete ACLs • Deploy Configuration File • Discover Driver • Deploy Passwords • Reboot Device • Run Command Script • Run Diagnostics • Run ICMP Test • Synchronize Startup and Running • Take Snapshot • Update Device Software If checked, the above tasks enable users to select the task owner's AAA credentials to use when running the task. (**Note**: The user must have valid AAA credentials defined.) For information on per-task credentials, refer to "Per-Task Credentials" on page 52.
Fallback Admin User	Enter an Admin user whose AAA credentials are used for tasks with unknown users.
Nortel Discovery	
Nortel BayRS MIB/ OS Versions	Displays a list of additional BayRS MIB versions/revisions that will discover the BayRS driver. Use <MIB Version>/<Revision> sequences separated by vertical bars, for example: 14.00/1D12|14.20/).
Gateway Mesh	
Local Gateway Host	Enter the hostname or IP address and port of the Gateway system that is in the same Realm as the NA Core (for example: `gw-vlan10:3001`). For information on the Gateway Mesh, refer to "Overlapping IP Networks" on page 153.
Local Gateway Proxy Port	Enter the port name of the Gateway system that is in the same Realm as the NA Core (for example: `gw-vlan10:3001`). The default is 3002. For information on the Gateway Mesh, refer to "Overlapping IP Networks" on page 153.
Local Gateway Admin Port	Enter the Admin port number for the Gateway in the local Realm. This is used to fetch the Realm names from the Gateway Mesh. The default is 9090.

Field	Description/Action
Gateway Admin Private Key Filename	Enter the filename of the private key for the Gateway needed to connect to the Admin port. This can be an absolute path or a relative path. A relative path is relative to the root of the NA install tree, typically *C:\NA*. Keep in mind that the private key for the Gateway is created when the Gateway is installed. When using a NA Standalone Gateway, the private key filename is `opswgw-mngt-server.pkcs8`. This file must be copied from the *saOPSWgw*/certificates* directory where the NA Gateway was installed. This file should be copied to the root of the NA installation, typically *C:\Rendition*. If you are integrating NA with HP SA, NA uses the HP SA Gateway Mesh. In this case, copy the `spog.pkcs` file from the HP SA host to the root of the NA installation, typically *C:\Rendition*. Be sure to change the filename in the Admin Settings to `spog.pkcs8`. **Note**: The `.pcks8` file is a PKCK#8 format file containing a private key used in a public key encryption scheme. To secure the Gateway Mesh, the private key must be used to administer the Gateway Mesh. NA uses the Gateway Mesh administration function to list the Realm names supported by the Gateway Mesh. To test the Gateway Admin settings, open the New Device page and scroll down to the Connection Information section to see that there is a Realm name list.
Gateway Mesh Delay	Enter the number of seconds of latency to reach remote Realms through the Gateway Mesh. The default is five seconds. This number is added to the time-outs used when communicating with remote devices.

Be sure to click Save to save your changes.

Per-Task Credentials

Configuring per-task credentials enables you to specify what credentials are used to access devices by specifying unique credential handling for tasks that access devices. You can:

- Run tasks using the AAA credentials of the task owner
- Run tasks using one-time credentials specified when the task is created
- Configure which types of tasks require which types of credentials

Typically in a secure environment, you might have implemented a AAA server, such as CiscoSecure ACS TACACS+ server, that limits which commands each user is allowed to run on each device.

For example, suppose both User A and User B can run command scripts using specific commands for which they have permissions. Once NA is implemented, both User A and User B need to be able to run commands scripts. However, you want to ensure that both User A and User B maintain credentials to run only the commands for which they have permissions.

Consequently, when using per-task credentials, you do not have to set up a new, static NA account for User A and User B with permissions to run commands scripts. Each user can run command scripts with their current permissions. If either User A or User B uses a command for which they do not have permissions, NA will return an error.

When using AAA credentials, NA:

- Tries all standard credentials processing, including Last Successful Credentials, Device-Specific Credentials, Password Rules, and Device Archived Passwords.
- For each attempt, NA replaces the username and password with the task owner's AAA username and password. If an attempt fails, NA will retry again with the user's AAA password as both the exec and enable password. If all AAA login attempts fail, the task will fail.

Note: There is a hidden config setting proxy/auth_fallback_for_aaa_task that can be set in an .RCX file. If set to true, NA will fall-back and attempt standard password handling.

When configuring one-time credentials, NA uses the specified type of credential handling, based on its task type. For example, if only AAA credentials are allowed for Snapshot tasks, all snapshot task will use AAA credentials. If more than one credentials type is allowed for a given task type, the user has a choice as to which to use.

If a given task is selected to use one-time credentials, NA uses the exact credentials specified by the user when the task was created. If the one-time credentials fail, the task fails.

Note: If the one-time credentials succeed, NA does not update the last successful credentials information for the device.

Server

The Server page enables you to:

- Designate TFTP, FTP, and SMTP servers
- Set NA task limits
- Configure Syslog
- Configure device importing intervals
- Configure Primary IP address reassignment and deduplication settings
- Configure Domain Name resolution
- Enable the Audit Log
- Configure database pruning
- Configure advanced scripting capabilities
- Configure HTTP Proxy Servers
- Configure dynamic device group re-calculation
- Configure software image management
- Specify the absolute path to the directory of the extension drivers
- Configure server performance tuning
- Configure event differencing size thresholds
- Ignore Syslog change detection on non-managing NA Cores

To view the Server page, on the menu bar under Admin, select Administrative Settings and click Server. The Server page opens.

Server Page Fields

Field	Description/Action
Servers	
FTP/TFTP Server IPv4 Address	Enter the IPv4 address of the FTP/TFTP server used by NA (by default, the NA server itself).
FTP/TFTP Server IPv6 Address	Enter the IPv6 address of the FTP/TFTP server used by NA (by default, the NA server itself). For detailed information on IPv6 support, see the *NA Installation and Upgrade Guide*.
FTP/TFTP File Path	Enter the path and folder to which the FTP/TFTP server writes the configuration files. NA requires read/write permissions to this folder. The default is *C:\<install directory\server\ext\tftp\tftpdroot.*
Syslog Server IPv4 Address	Enter the IPv4 address of the Syslog server used by NA. (**Note**: When not specified, the first non-loopback IPv4 address of the NA server is used.)

Field	Description/Action
Syslog Server IPv6 Address	Enter the IPv6 address of the Syslog server used by NA. (**Note**: When not specified, the first non-loopback IPv6 address of the NA server is used.)
SMTP Server	Enter the host name or IP address of the SMTP server NA uses to send email notifications.
SMTP From Address	Enter the From address NA uses for email.
Tasks	
Max Concurrent Tasks	Enter the maximum number of tasks that can run simultaneously. This setting limits the number of non-group tasks that can run simultaneously. NA limits the number of concurrent non-group tasks to avoid hindering system and network performance. The default is 20 concurrent non-group tasks. Keep in mind that there is a limit to the number of database connections in the database connection pool. For the recommended values of Max Concurrent Tasks, see the *NA Support Matrix*. **Note**: NA runs only as many tasks as can be supported by the current NA server configuration. If there is insufficient memory to run the number of tasks configured by Max Concurrent Tasks, NA runs only as many tasks as the available memory can support.
Max Concurrent Group Tasks	Enter the maximum number of tasks that can run simultaneously. This setting limits the number of non-group tasks that can run simultaneously. NA limits the number of concurrent non-group tasks to avoid hindering system and network performance. The default is 20 concurrent non-group tasks. Keep in mind that there is a limit to the number of database connections in the database connection pool. For the recommended values of Max Concurrent Tasks, see the *NA Support Matrix*. For additional considerations, see “Tuning the NA Management Engine” in the *NA Administration Guide*. **Note**: NA runs only as many tasks as can be supported by the current NA server configuration. If there is insufficient memory to run the number of tasks configured by Max Concurrent Tasks, NA runs only as many tasks as the available memory can support. For information about the current health of the NA task subsystem, see “Viewing Task Load” on page 411.
Max Task Length	Enter the maximum time a task can run before it is stopped and given a Failed status. The default is 3,600 seconds (one hour). When the “Max Task Length” time period is reached for a given task, NA attempts to stop the task. The task will not actually stop processing, however, until it reaches a point where it can safely stop. Note that for some tasks, this could take a significant amount of time.
Syslog Configuration	
Configure Syslog by Default	If checked, NA automatically configures Syslog change detection on new devices.
Default Syslog Relay	Enter the default host name or IP address of the relay host for new devices.
Device Import	

Field	Description/Action
Overwrite Existing Devices	Select one of the following options: • Yes — NA overwrites existing device data stored in the NA database with the data you import. Devices not included in the import are unaffected. • No — NA does not overwrite existing device data stored in the NA database with the data you import.
Missing Device Interval	Devices that are missing from an import source longer than this interval are deleted, marked inactive, or left unchanged (per the Missing/Inaccessible Device Action). The default is 45 days.
Inaccessible Device Interval	Any device that NA cannot access in this interval is deleted, inactive, or left unchanged (per the Missing/Inaccessible Device Action). The default is 45 days.
Missing/Inaccessible Device Action	Select one of the following options: • Delete device — Deletes devices that are missing or inaccessible from the database. • Mark device inactive — Marks missing or inaccessible devices as inactive (the default). In general, it is a good idea to change devices to inactive rather than deleting them from the database to preserve the configuration history • No action — No action is taken for missing or inaccessible devices.
User Import	
Overwrite Existing User or User Group	Select one of the following options: • Yes — NA overwrites existing user account and user group data stored in the NA database with the data you import. User accounts and user groups not included in the import are unaffected. • No — NA does not overwrite existing user account or user group data stored in the NA database with the data you import.
Primary IP Reassignment and Deduplication Settings	
Primary IP Address Reassignment	If checked, NA looks through all IP addresses associated with the device, including the primary IP address (plus all other interfaces associated with the device), and sets the primary IP address that matches a RegEx or other rule, if provided.
Interface Name Reassignment RegEx Patterns	Enter a Regular Expression (RegEx) patterns in the right-hand box and click the Add Pattern << pattern. A regular expression is a special text string to specify the interface name (for example: Loopback.*) to which an IP address must conform. To delete patterns, select the patterns from the left-hand box and click the Delete Pattern button.
IP Address Reassignment RegEx Patterns	Enter a Regular Expression (RegEx) patterns in the right-hand box and click the Add Pattern << button. A regular expression is a special text string to match IP addresses on available interfaces (for example: 10\.1\..*). To delete patterns, select the patterns from the left-hand box and click the Delete Pattern button.
IP Reassignment Order	If more than one IP address matches the interface names or IP address patterns, select either: • Lowest IP address to assign as the primary IP address (the default) • Highest IP address to assign as the primary IP address

Field	Description/Action
Duplication Detection	Select one of the following options for devices when duplicates are detected. **Note**: Devices are considered duplicates if they have the same interface and IP address information. • Leave Duplicates • Deactivate Duplicates (the default) • Delete Duplicates
Domain Name Resolution	
Overwrite Existing Domain Names	If checked, NA overwrites manual FQDN entries with DNS-resolved FQDN entries when you run a Resolve FQDN task. Keep in mind that when the task is run, both the Device Domain Name and the Device Hostname are replaced.
Audit Log	
Audit Logging	Select one of the following options: • Enabled — NA stores an audit log of user actions. Click View Audit Log to see the log. • Disabled — NA does not store an audit log of user actions (the default).
Database Pruning	
Configurations	Enter the number of days to save configurations in the database. The default is 365 days.
Diagnostics	Enter the number of days to save diagnostics in the database. The default is 45 days.
Events	Enter the number of days to save events in the database. The default is 45 days.
Tasks	Enter the number of days to save tasks in the database. The default is 365 days.
Sessions	Enter the number of days to save proxy Telnet/SSH sessions in the database. The default is 45 days.
Log Files	Enter the number of days to save server log files. The default is 30 days. Log files can get very large, so pruning them can be vital to freeing up disk space on your server.
Temporary Driver Files	Enter the number of days to save temporary driver files. The default is 30 days.
Task Log Files	Enter the number of days that task log files will be retained. The default is 7 days.
Topology Data	Enter the number of days to save topology data. The default is 45 days.
Diagram Files	Enter the number of days to save diagram files. The default is 1 day.
ACL Data	Enter the number of days to save ACL data. The default is 365 days.
Device Authentication Data	Enter the number of days to save Device Authentication data. The default is 45 days.

Field	Description/Action
Advanced Scripting	
Scripting Language 1	Advanced Scripting enables you to run custom scripts written in the scripting languages used in your network. You must have the language interpreter for each language installed and then associate the path with the language option via the Advanced Scripting settings. The scripting language specified here appears in a selection list on the New Command Script page when the Advanced Scripting option is enabled. By default, this setting is pre-configured for Expect. You must specify the path to the interpreter for this language in the corresponding Path to Interpreter [#] setting on this page. You can configure Advanced Scripting capability for up to five languages, and you can overwrite the pre-configured defaults if you do not use those languages. Only languages that run from the command line are supported (for example, JScript and Python). **Note**: Slots 1 and 2 are pre-configured for Expect and Perl. However, NA installs only the interpreter for Expect. You must install the interpreter for each language you specify here, and configure the path before you can run scripts written in these languages.
Path to Interpreter 1	Enter the path to the interpreter that runs the language specified in Scripting Language 1.
Scripting Language [2-5]	The language specified here is displayed in the Language selection list on the New Command Script page when the Advanced Scripting option is enabled. You must specify the path to the interpreter for this language in the corresponding Path to Interpreter [#] setting. **Note**: By default, Scripting Language 2 is pre-configured for Perl, but you must install the Perl interpreter for this setting to function.
Path to Interpreter [2-5]	Enter the path to the interpreter that runs the language you specified in the associated Scripting Language [#] box. **Note**: For Windows environments, by default Path to Interpreter 2 is pre-configured for Perl, but NA does not install the Perl interpreter. Perl must be installed and the path configured for this setting to function.
Dynamic Groups	
Dynamic Group Auto-Recalculation	Enter how frequently the system re-calculates the member devices of all dynamic groups. The default is 60 minutes. Enter 0 to disable Auto-recalculation. (**Note**: Re-calculating dynamic group members means NA will do number of queries to determine which devices belong to the dynamic group, based on the group's rules and/or filters.)
Event Driven Recalculation	If checked, the system will re-calculate all dynamic group members each time a device change event occurs.

Field	Description/Action
Device Change Events	Select the device change events that will trigger dynamic group member re-calculation. This setting is in effect only when the Event Driven Recalculation option is enabled. Examples of device change events include: • Device Added • Device Configuration Change • Device Deleted • Device Edited • Device Software Change • Device Unmanaged
Software Image Management	
SNMP Retry	Enter how many attempts should be made after the initial failed attempt. The maximum is five.
SNMP Timeout	Enter the timeout for SNMP packets in seconds. The default is five.
Telnet Timeout	Enter the socket timeout value in seconds. The default is 10.
HTTP Proxy Server	Enter an HTTP Proxy server. A Proxy server is used to access Cisco.com via HTTP if direct access does not work.
HTTP Proxy Server Port	Enter the HTTP Proxy server's port.
Software Image Management Service Host	Enter the Hostname or IP address of the system running the Software Image Management service.
Software Image Management Service Port	Enter the Software Image Management service port. This is the port the Software Image Management service is listening on. Typically this is port 6099.
Drivers	
Driver extension directory	Enter the directory where NA should look for any additional drivers. Refer to your Driver Development Kit (DDK) documentation for information on developing drivers.
Performance Tuning	
For a list of events, refer to "Getting Started" on page 456.	Click the check box for each event you want to filter. This enables you to tune the performance of your system. You can also limit event differencing for large configs, limit line-by-line masking for large configs, limit storage and display of large task session logs, and so on.
Special Performance Settings	
Limit event differencing for large configs	For very large configurations, the process of creating the configuration difference report in an event e-mail can consume a large amount of system resources. Enabling this option and setting a size limit (see below) will cause the configuration difference report to be skipped for events where the configuration size is greater than the specified threshold.
Event differencing size threshold	Setting a size limit will cause the configuration difference report to be skipped for events where the configuration size is greater than the specified threshold.

Field	Description/Action
Limit line-by-line masking for large configs	For very large configurations, the process of showing the line-by-line differences between two configurations can consume a large amount of system resources. Enabling this option and setting a size limit (see below) will cause the configuration differences page to show the two configurations side-by-side without any additional highlighting or line numbering for those configurations with a size greater than the specified threshold.
Line-by-line masking size threshold	Setting a size limit will cause the configuration differences page to show the two configurations side-by-side without any additional highlighting or line numbering for those configurations with a size greater than the specified threshold.
Limit storage and display of large task session logs	Task session logs are stored as part of the task results. Some devices dump large amounts of data into the session log, resulting in a significant increase in the size of the task table in the database. Enabling this option and setting size limit (see below) causes the session logs to be truncated once the specified threshold is met, ensuring that session logs never grow too large.
Task session log size threshold	Setting a size limit causes the session logs to be truncated once the specified threshold is met, ensuring that session logs never grow too large.
Ignore Syslog Change Detection on non-Managing Cores	In a Distributed System, if devices are setup to send Syslog messages to multiple NA Cores, database replication conflicts can occur when both NA Cores try to schedule Snapshot tasks for the same device at the same time. Enabling this option instructs the NA Core to ignore the Syslog message and not schedule the Snapshot task. For information on Distributed Systems, see the *NA Multimaster Distributed System on Oracle Guide*.
Allow a core or cores in the mesh to run all tasks created on that core locally	This option instructs the local NA Core that tasks for a given device can run on any NA Core, so to ensure that only one task at a time runs on any device. This NA Core must communicate with the other NA Cores to determine what tasks are running. For information on Distributed Systems, see the *NA Multimaster Distributed System on Oracle Guide*.
Allow this core to run all tasks created on it locally	This option causes any tasks created by a user logged into this NA Core to assign tasks to the current NA Core. This ignores the managing NA Core for the site to which the device belongs. For information on Distributed Systems, see the *NA Multimaster Distributed System on Oracle Guide*.

Be sure to click Save to save your changes.

Workflow

The Workflow page enables you to:

- Enable Workflow
- Configure event notification and response rules
- Configure the Device Reservation System
- Configure Device Reservations for the Telnet/SSH Proxy

To view the Workflow page, on the menu bar under Admin, select Administrative Settings and click Workflow. The Workflow page opens.

Workflow Page Fields

Field	Description/Action
Workflow	
Enable Workflow	If checked, approval is required for tasks for which an Approval rule is defined.
Priority Values	Defines the priority values that can be set on tasks requiring approval. The default values include: • Low • Medium • High You can add different values, such as Urgent, Normal, and so on by entering the value and clicking the Add Value << button. You can delete a value by selecting the value and clicking Delete Value button. **Note**: The NA Scheduler does not look at the values. It is basically a visual queue for you to determine which tasks need approval in a timely manner.
Event Notification & Response Rules	
Run Task	If checked (the default), all tasks that are scheduled due to event rules must be approved. For example, if a configuration policy non-compliance event occurs, thereby triggering a task for corrective action, the task must be approved before deployment.
Device Reservation System	
Device Reservation System	Select one of the following options: • Enabled — Enables the Device Reservation System (the default). For information on the Device Reservation System, refer to “Reserving Devices” on page 192. • Disabled — Disables the Device Reservation System.
Default Duration	Enter the number of minutes devices and/or device groups can remain reserved. The default is 60 minutes.
Max Number of Columns in Activity Calendar	Sets the maximum number of columns in the Activity Calendar. The default value is 1024. For information on the Activity Calendar, refer to “Activity Calendar” on page 193.

Field	Description/Action
Minimum Overlap for Half-Hour	Set the minimum number of minutes into a half-hour a reservation must extend for it to be displayed on the Activity Calendar as reserved for that half-hour. The default value is 5 minutes.
Telnet/SSH Proxy Reservation	
Device Reservations for Telnet/SSH Proxy	The NA Telnet/SSH Proxy can be used to access and configure devices. It provides access control, keystroke session logging, and in-line commenting capabilities. Select one of the following options: • Ignore — Ignore device reservations when accessing devices via the Telnet/SSH proxy (the default). For information on the Device Reservation System, refer to "Reserving Devices" on page 192. • Warn — Warn users if an approved device reservation does not exist when connecting to a device via the Telnet/SHH proxy. • Prevent — Prevent users from connecting to a device via the Telnet/SSH proxy if an approved device reservation does not exist. If the user has Override permission, he/she is prompted as to whether or not to override non-access to the device. If Warn or Prevent is selected, NA looks for a matching device reservation, including user, device or device group, if approved, and the time reserved for the multi-task project.
No Device Reservation Warning Message	Enter the warning message to display when an approved device reservation does not exist. The default warning message is: *WARNING: You do not have an approved reservation for this device at this time*. You have the option of deleting the default warning message.

User Interface

The User Interface page enables you to:

- Configure login security
- Set the date format shown on all pages
- Customize NA menus
- Add slots for the View/Edit Modules pages
- Add and delete roles from the New/Edit Templates pages
- Customize the size of the text box on the Edit Command Script Diagnostic pages
- Customize the Device Selector display
- Enable enhanced custom fields
- Configure Quick Launch tasks

To view the User Interface page, on the menu bar under Admin, select Administrative Settings and click User Interface. The User Interface page opens. Be sure to click Save when you are done.

User Interface Page Fields

Field	Description/Action
Security	
Session Timeout	Enter the number of seconds NA waits before terminating an inactive Web session. The default is 1800 seconds. Keep in mind that the change will not take effect until your next login.
Check Device Permissions for View Device Configuration	If checked, users can view the device configuration only if they have appropriate device permission. You must restart NA for your change to take effect.
Auto-complete user name and password	If checked, the browser's auto-complete function is enabled on the NA login page.
Show Stack Traces	If checked, exception stack traces can be viewed in the Web UI error page.
Cross site scripting check	If checked, NA checks user input to filter out the potential cross site scripting elements such as <script>, <object>, <img>, <input>, and so on. In other words, this option enables you to remove potentially malicious Javascript code from your scripts. An error is returned when malicious Javascript code is found.
Date/Time Display	
Date Format	This setting controls how dates appear throughout the Web interface. The default format is MMM-dd-yy HH:mm:ss. You can vary the order of the date and time elements, swap the date and time, enter a 4-digit year (yyyy), and change the month to a 2-digit numeric value (MM). Keep in mind that the elements are case-sensitive. For example HH refers to a 24-hour clock, while hh refers to a 12-hour clock.

Field	Description/Action
Menu Customization	
Show Custom Menu Link	If checked, a user-defined name appears above the About option. You provide the menu title and link to an HTML page, such as the home page of your ticketing application.
Custom Menu Title	Enter the name you want to appear.
Custom Menu Page	If Show Custom Menu Link is selected, enter the URL to the HTML page you want to display when a user clicks the menu title. This can be a page within another HTML application.
Configuration Comparison	
Lines of Context for Visual Comparison	Enter the number of lines to display above and below each change when comparing two configurations. The default is 3.
Lines of Context for Email Comparison	Enter the number of lines to display above and below each change when comparing two configurations as text in email. The default is 3.
Software Center	
Slots	Add and delete the slots (chassis slots for cards/blades/modules) that users see on the View/Edit Modules pages. To add a slot, enter it in the right-hand box and click Add Slot <<. To delete a slot, select the slot in the left-hand box and click Delete Slot.
Show file compliance level	Select the checkbox to display the compliance level for each Image file in the Image Sets.
Device Models	Enter a device model and then click the Add Model button. The Delete Module button enables you to delete device modules.
Processor Types	Enter a processor type and then click the Add Processor button. The Delete Processor button enables you to delete processor types.
Device BootROM	Enter a Device BootROM and then click the Add Device BootROM button. The Delete BootROM button enables you to delete Device BootROMs.
Templates	
Template Roles	Add and delete the roles that template authors choose from on the New/Edit Template pages. Roles can describe the role devices play in your network, such as Border or Core. To add a role, enter it in the right-hand box and click Add Role <<. To delete a role, select the role in the left-hand box and click Delete Role.
Scripts	
Script Text Height	Enter the size (height) of the text box on the Edit Command Script and Edit Diagnostics pages. The default is 12 rows.
Script Text Width	Enter the size (width) of the text box on the Edit Command Script and Edit Diagnostics pages. The default is 60 characters.
Enhanced Custom Fields	
Enable Enhanced Custom Fields	If checked, you can configure enhanced custom fields for some data sets. Custom data fields enable you to assign useful data to specific devices, configurations, users, and so on. For more information, see "Enhanced Custom Fields Setup" on page 564.

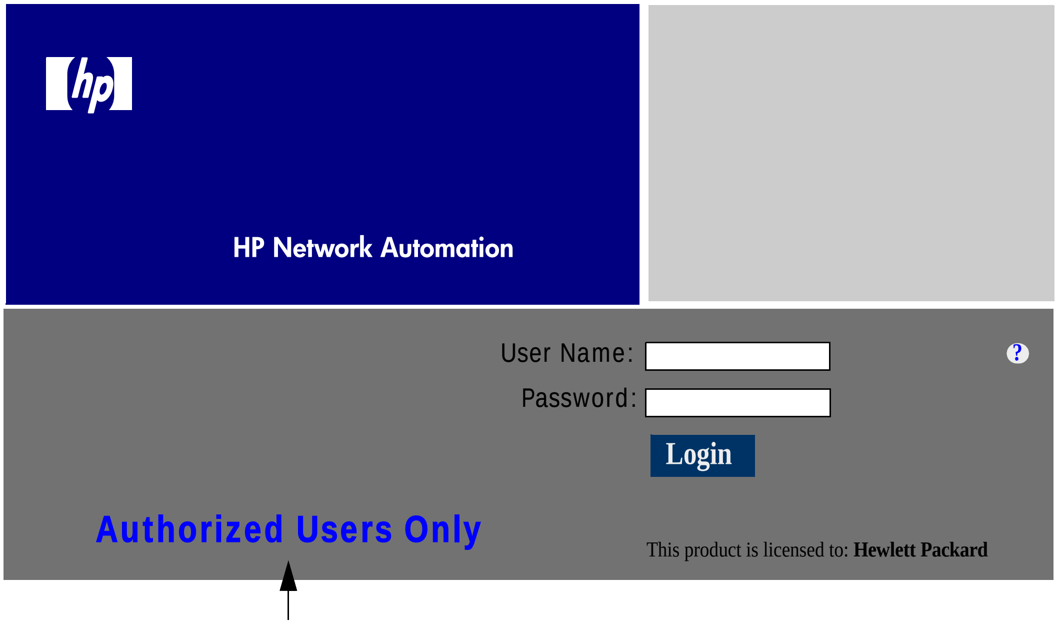
Field	Description/Action
Proxy Window	
Dimension of proxy window	Select the size to use for the proxy window.
Miscellaneous	
Task Page Refresh Interval	Enter the number of seconds for the Task List pages to refresh. The default is 60 seconds.
Config Size Threshold for Displaying as Plain Text	Enter a config size threshold for displaying a config in plain text. The default is 200,000 bytes. Keep in mind that certain configs are too large to provide special handling, such as line numbering, without consuming enormous server and browser resources. When a config exceeds the default value, it is displayed as plain text using <pre> and </pre> tags.
Mask Community Strings	If checked, community strings in the Web UI will not be shown in plain text. This option is for NA-displayed community strings only. Community strings embedded in configurations are masked based on driver-specific sensitive data masking implementation.
Disable hidden stack trace output	If checked, hidden stack trace is disabled. If not checked, when a server error occurs, NA outputs the stack trace as hidden text in the HTML page in addition to the server log. (**Note**: A full Java stack trace is provided as hidden HTML by default to aid in Support calls. If you think this might be a potential security vulnerability, check this option.
Disable detailed exception message output	If checked, output of the detailed exception message is disabled. If not checked, when a server error occurs, NA outputs a detailed exception message in the HTML page, in addition to the server log.

Customizing the NA Login Page

You can customize the HP Network Automation (NA) Login page to display information, such as a warning message or company-specific information.

To customize the HP Login page:

1. In the *$NA_HOME/resource* directory, open the *customer_banner.html* file. If the file does not exist, create one with that name. (Note: You may also need to create the *resource* directory.)
2. Open the file with a text editor that supports HTML, and then enter the text to be displayed on the NA logon page.
3. Save the file, and then log on to NA. The text is displayed under the Log In button. There is no limitation on the number of words you can display. However, you should check the display to make sure that it fits properly on the page.
   The following is a sample logon page.



Authorized Users Only

This product is licensed to: **Hewlett Packard**

Custom Banner

Telnet/SSH

The Telnet/SSH page enables you to configure:

- Telnet/SSH logging
- The Telnet/SSH proxy
- Device single sign-on
- The Telnet client
- The Telnet server
- The SSH server

To view the Telnet/SSH page, on the menu bar under Admin, select Administrative Settings and click Telnet/SSH. The Telnet/SSH page opens.

Keep in mind that all tasks that interact with a device can be run with session logging enabled. This provides a detailed log of the interaction with the device during the task. Session logs should be viewed as the first step to debugging device-specific issues. Session logs provide details on CLI, SNMP, and all transfer protocol actions taken during the task.

Telnet/SSH Page Fields

Field	Description/Action
Telnet/SSH Session Logging	
Log Commands	If checked, this option saves your commands when running a Telnet or SSH session. To view the commands, from the Device Information page, click View Telnet/SSH Sessions and then View Commands Only. The Convert to Script links on this page enable you to quickly capture the commands from a session into a script for future use. Refer to “Adding Command Scripts” on page 582 for information.
Log Responses	If checked, this option saves the complete session logs when running a Telnet or SSH session. To view the logs, from the Device Information page, click View Telnet/SSH Sessions and the View Full Session. The Convert to Script links on this page enable you to quickly capture the commands from a session into a script for future use. Refer to “Adding Command Scripts” on page 582 for information.
Force Logging	If checked, this option forces logging of device command and the responses for each Telnet/SSH session during API usage.
Telnet/SSH Proxy	
Enable Telnet/SSH Server	The Telnet/SSH Proxy can be used to access and configure devices. It provides access control, keystroke session logging, and in-line commenting capabilities. If checked (the default), NA can operate as a Telnet/SSH server.
Server Inactivity Timeout	Enter the maximum time an idle Telnet or SSH session is connected to the NA Telnet/SSH server before being disconnected. If a Telnet/SSH client connected to NA is not active for this period of time, the session times out. The default is 30 minutes.

Field	Description/Action
Default Connection Method	Select either Telent or SSH to connect to a device without Single Sign-on. This is the connection method used by the Telnet/SSH Proxy connect command when the -*method* option is not included. The method is ignored unless Use Single Sign-on is selected and the Edit Device page Supports list includes the same connection method. **Note**: When NA is configured to use SecurID for external authentication, Single Sign-on functionality will not be enabled when connecting to the NA proxy. You will need to authenticate again using your SecurID credentials because SecurID passcodes cannot be reused.
Device Inactivity Timeout	Enter the number of minutes NA keeps an idle device session open before closing the connection. The default is 30 minutes.
SSH Login Timeout	Enter the number of seconds for timeout of SSH logins using the “-login” switch in the NA proxy. The default is 15 seconds.
Alert for Concurrent Session	Select one of the following options: • Warn of Concurrent Sessions — If checked (the default), NA issues a warning when a second user tries to connect to a device. This helps prevent one user from inadvertently overwriting the changes of another. Only users with Admin permissions can override a warning. • Prevent Concurrent Sessions — If checked, NA prevents concurrent sessions for all users. • No Action — If checked, NA ignores concurrent sessions.
Concurrent Session Handling for Distributed System	Select one of the following options: • Allow sessions to non-local devices (Note that if both “Warn of Concurrent Sessions” (see above) and “Allow sessions to non-local devices” is checked, no warning is issued.) • Prevent sessions to non-local devices For information on Distributed Systems, see the *NA Multimaster Distributed System on Oracle Guide*.
Connect to Unknown Devices	If checked (the default), NA enables users to connect to unmanaged devices.
Max Device Connection List	Enter the maximum number of devices displayed when connecting to a device based on a wildcard search and multiple matching devices are found. The default is 20. If more devices can be returned, you are prompted to restrict the wildcard expression.
Device Single Sign-0n	
Use Single Sign-on	If checked (the default), NA automatically authenticates a user once, then logs them into devices for which they have modify device permissions. **Note**: When NA is configured to use SecurID for external authentication, Single Sign-on functionality will not be enabled when connecting to the NA proxy. You will need to authenticate again using your SecurID credentials because SecurID passcodes cannot be reused.

Field	Description/Action
Sign-On Mode When No Modify Device Permission	Select one of the following options: • Provide Login Prompt • Sign On To Limited Access Mode • Deny Login
Display Sign-on Banner	If checked (the default), NA displays the sign-on banner when it logs into a device.
Use AAA Login for Single Sign-on	If checked, NA uses the AAA login information. This option refers to the Use AAA Login for Proxy Interface section on the New/Edit User page.
Use HP Network Automation Login when AAA Login Fails	If checked (the default) and your AAA user name and password information fails, your NA login information is used.
Telnet Client	
Telnet Client	Select one of the following options: • Use NA's integrated telnet client (the default) (**Note**: This is the only option that supports single-sign on.) • Use standard browser telnet:// URL to NA’s telnet proxy • Use standard browser telnet:// URL directly to the indicated device
Telnet Server (changing these setting restarts the Telnet/SHH server)	
Enable Telnet	If checked (the default), NA acts as a Telnet server.
Telnet Server Port	Enter the port on which NA accepts client connections. The default for Windows is 23. The default for UNIX® is 8023.
Max Telnet Connections	Enter the maximum Telnet client connections NA accepts simultaneously. The default is 50.
SSH Server (changing these setting restarts the Telnet/SHH server)	
Enable SSH	If checked (the default), NA acts as an SSH server.
SHH Server Port	Enter the port on which NA accepts client connections. The default is 22.
Max SSH Connections	Enter the maximum SSH client connections NA accepts simultaneously. The default is 50.

Be sure to click Save to save your changes.

Reporting

The Reporting page enables you to customize the Network Status Report for your organization, including:

- Policy Rule Violations
- Software Compliance Violations
- Startup vs. Running Config Mismatch
- Device Access Failure
- Configuration Change
- Email Report
- Diagramming
- Image Synchronization Report

For each reporting category, you can set status indicators for individual devices (and for the device group) using a combination of risk level color codes and parameters that specify a threshold for the percentage of devices that are out of compliance at each tier. For example, a higher score might be assigned to the border routers group, which control external network access and remote offices, while LAN devices might remain at the default values.

Providing settings that best reflect the significance of each event in your network can help you identify problems and keep the network in compliance with all established policies practices.

The Reporting page also provides options for the format and content of email reports sent via a user-defined email notification task and for specifying the location where you want to save the reports. You can also enable diagramming and set diagramming parameters. For information on Diagramming, refer to “Diagramming Page Fields” on page 614.

Note: The status (risk level) of a non-complying device determines the status of the group. For example, if you set the risk level for a single non-compliant device to yellow, and one device in a group is in violation, the device group will reflect status yellow when the threshold number of devices in violation is reached.

To view the Reporting page, on the menu bar under Admin, select Administrative Settings and click Reporting. The Reporting page opens.

Reporting Page Fields

Field	Description/Action
Policy Rule Violations	
Device Status Color	Select the color to display when a single device in a device group is in violation of a configuration policy rule. The options include: • Red (the default) • Yellow • Green
Category Status Color	Enter the threshold percentage of devices that have configuration policy violations for the following device status colors: • Yellow — The default 1%. • Red — The default is 2%.
Software Level Violations	
Device Status Color	Select the color to display when the software for a single device in a device group is out of compliance. The options include: • Red (the default) • Yellow • Green The following compliance levels are considered to be violations: • Security Risk • Pre-production • Obsolete • Bronze • Silver • Gold • Platinum
Category Status Color	Enter the threshold percentage of devices that have software level violations. The options include: • Yellow — The default 1%. • Red — The default is 2%.
Startup vs. Running Config Mismatch	
Device Status Color	Select the color to display when the startup configuration of a single device in a device group does not match its running configuration. The options include: • Red • Yellow (the default) • Green

Field	Description/Action
Category Status Color	Enter the threshold percentage of devices that have startup versus run mismatches. The options include: • Yellow — The default 1%. • Red — The default is 2%.
Device Access Failure	
Device Status Color	Select the color to display when a single device in a device group reports a device access failure. The options include: • Red • Yellow (the default) • Green
Category Status Color	Enter the threshold percentage of devices that have access failures. The options include: • Yellow — The default 1%. • Red — The default is 2%.
Configuration Change	
Device Status Color	Select the color to display when the configuration of a single device in a device group has changed. The options include: • Red • Yellow (the default) • Green
Category Status Color	Enter the threshold percentage of devices that have configuration changes. The options include: • Yellow — The default 1%. • Red — The default is 2%.
Email Report	
Email Report Format	Select the email format you want to use when sending search results as an email report. Keep in mind that this does not apply to Network Status reports. Options include: • HTML mail (the default) • CSV file attachment • Plain text • HTML mail (without links)
Include Task Results in Email Reports	If checked, complete task details are included in email reports that contain the results of a task search in comma separated value (CSV) file format. Keep in mind that this does not apply to Network Status reports.

Field	Description/Action
Email Links	Select the format of addresses for HTML links in an email report. Options include: • Hostname (if resolvable) • IP Address • Canonical Name (FQDN, if resolvable) (the default) • User Defined — Enter the user-defined server address to use in email links.
SingleView	
Device Change Events to Track	Select the device change events to track. This setting determines the default set of events to display on the Single View page. Refer to “SingleView Page Fields” on page 553. Events include: • Device Configuration Change • Device Booted • Device Diagnostic Changed • Device Password Change • Module Added • Module Changed • Module Removed • Software Change • User Message
Diagnostics to Track	Select the diagnostics to track. This setting determines which Device Diagnostic Changed events are displayed if that event type is selected on the Single View page. Refer to “SingleView Page Fields” on page 553. Default diagnostics types include: • Hardware Information • Memory Troubleshooting • NA Detect Device Boot • NA Device File System • NA Flash Storage Space • NA Interfaces • NA Module Status • NA OSPF Neighbors • NA Routing Table **Note**: For detailed information on diagnostics, refer to “View Menu Options” on page 203.
Diagramming	
Enable Diagramming	If checked, enables the diagramming functionality.

Field	Description/Action
Maximum Nodes	Enter the maximum number of nodes to display in the diagram. The default is 250 nodes. This value can be lowered if generating the diagram is causing “Out of Memory” errors. Diagrams that include a large number of nodes result in large images. Images are generated in memory in uncompressed form before being output in JPEG format. You can increase the value if you want to include more nodes in your diagram, but keep in mind that you could run out of memory.
Label Font Size	Enter the font point size for labels in the diagram. The default is 8. Increasing this value increases the size of the labels in relation to the size of the nodes, potentially making the labels more readable.
Maximum Layout Duration	Enter the maximum time for which the layout algorithm is to run. The default is 30 seconds. The layout algorithm will stop after this maximum amount of time. Keep in mind that an accurate diagram is still generated if this limit is reached. However, the diagram might not be as optimally laid-out as possible.
Diagram Compactness	Enter the amount of space shown between nodes, from 0 to 100. The default is 95. This value controls how spread out the diagram appears. Nodes on a less compact diagram are easier to read. While a more compact diagram uses less space, compact diagrams can be hard to read. Also keep in mind that compact diagrams can take slightly longer to run, since the layout tends to take longer.
Quality-Time Ratio	Enter the preferred layout ratio from 0 to 100. The default is 100. Higher values generate a cleaner looking diagram, but take longer to layout and use more CPU cycles.
Preferred Edge Length	Enter a preferred edge length value, from 0 to 100. The default is 100. In general, longer edges provide more space between nodes in the diagram, however the layout algorithm will override this setting as needed. Larger values will cause the diagram to be more spread out, making memory consumption higher. Higher values do make edges less likely to overlap nodes and labels, thereby making the diagram more readable.
Preferred Minimal Node Distance	Enter a preferred minimal node distance value, from 0 to 100. The default is 20. This value controls how close nodes without connections are spaced. Smaller values contribute to a more compact diagram.
Image Synchronization Report	
Image Synchronization Report Files	Enter an Image Synchronization report file and click the Add Files button. The Delete Files button enables you to delete Image Synchronization report files. The Image Synchronization report enables you to view the currently running or backup software images on a device, or group of devices, that do not reside in the NA software image repository. For information on the Image Synchronization report, refer to “Image Synchronization Report Fields” on page 624.
Other	
Use Excel CSV Format	If checked (the default), when exporting search results to a comma separated value (CSV) file, Microsoft Excel CSV format is used.
Email Report File Export Location	Enter the path to the location on the NA server where you want all report files to be saved. All reports are automatically saved to this location when the user selects the “Save this report to file” option when defining the Email Report task. The default location is *C:\<install directory>/addins*.

User Authentication

User authentication enables you to centralize the authentication of users in one place and eliminate the need to maintain multiple databases. The following user authentication options are available:

- LDAP (Lightweight Directory Access Protocol)
- SecurID
- TACACS+
- RADIUS
- HP Server Automation (HP SA)
- HP Operations Orchestration (HP OO)

Keep in mind that if external authentication fails, NA attempts to fall-back to the local user credentials in the following cases:

- When the external authentication service is down or inaccessible.
- For static user accounts that have never successfully logged in via an external authentication method.
- For the built-in Admin user account.

Note: If you want NA to fail over to local authentication, you must enable this capability on the user's account. By default, NA will not fail over to local authentication. Refer to "Authentication Failover" on page 75 and to "New User Page Fields" on page 249 for information.

User authentication also enables you to configure the following security policies for built-in users within NA:

- Define a minimum password length
- Define password complexity rules
- Lock out users after a configured number of consecutive failed login attempts

To view the User Authentication page, on the menu bar under Admin, select Administrative Settings and click User Authentication. The User Authentication page opens. Refer to "User Authentication Page Fields" on page 79 for information.

Authentication Failover

When NA is configured to use an external application for user authentication, NA can fail over to local (NA application server) authentication in certain cases.

NA attempts authentication failover for the following users:

- The administrator user account (UID = 1) created at NA installation.
- Any user account that is configured for failover. (The External Auth Failover checkbox is selected on the New User or Edit User page.)

If external authentication does not succeed, NA uses the following algorithm:

- If NA cannot connect to the external authentication application, NA attempts local authentication if the user attempting to log on to the NA console is UID = 1 or is configured for authentication failover. If the user is not configured for authentication failover, NA does not attempt local authentication and returns a normal authentication error.
- If NA connects to the external authentication application but that application returns an error, NA attempts local authentication if the user attempting to log on to the NA console is UID = 1. For any other users, NA does not attempt local authentication and returns a normal authentication error.
- For LDAP authentication only, if the user attempting to log on to the NA console does not exist in the directory service, NA attempts local authentication.

LDAP Authentication

If your organization uses Microsoft Active Directory or LDAP (Lightweight Directory Access Protocol), you can import both your groups and users into NA. NA maintains active contact with your LDAP database, remaining current on who can and cannot log into applications.

Even when external user authorization is enabled, it is possible to login to NA if network problems make the LDAP server unreachable. If NA cannot connect to the designated LDAP server, users who have previously logged in to NA can login to NA using their NA user password. You can setup a NA password on the My Profile page. Refer to “My Profile Page Fields” on page 262 for information.

Make sure that no LDAP user has the same username as the NA System Administrator. The default System Administrator's username is “admin,” but it can be changed. If there is a name conflict between the default administrator and another LDAP user, it may prevent the default administrator from logging in to NA.

If a user is created in NA and deleted in LDAP, that user can login to NA again using his/her NA password (not LDAP password).

For information on setting up external authentication for LDAP, refer to “LDAP External Authentication Setup” on page 82.

SecurID Authentication

The RSA SecurID solution is designed to protect your organization by helping to ensure that only authorized users are granted access to networked resources. In general, SecurID is a two part authentication scheme, requiring a password/PIN, along with a token. The token changes every 60 seconds. Refer to “Adding SecurID Software Tokens” on page 636 for information.

TACACS+ Authentication

Cisco IOS software currently supports several versions of the Terminal Access Controller Access Control System (TACACS) security protocol, including TACACS+. TACACS+ provides detailed accounting information and flexible administrative control over authentication and authorization processes.

Using your TACACS+ server (typically CiscoSecure ACS) to authenticate users provides the following benefits:

- NA users need only remember a single username and password
- NA user administration can be centralized on the ACS server
- TACACS+ password restrictions can be easily enforced

Using your TACACS+ server to authenticate users into NA enables you to:

- Configure NA to use a TACACS+ server to authenticate user logins (i.e., to verify that the user has entered a valid username/password pair).
- Support TACACS+ authentication for the Telnet/SSH Proxy.
- Assign individual users a fallback password in NA.
- Identify TACACS+ users so their fallback password is only used when the TACACS+ server is inaccessible (but not if any user other that Admin has entered an invalid TACACS+ password).
- Configure multiple TACACS+ servers for fail-over purposes.

Keep in mind that NA needs to be defined in TACACS+ as an authenticating device, similar to any other router, along with a specific username. This enables users to login to NA and NA to login to their network devices.

Note: TACACS+ is not used for authorization/permissions. This means that the user must be added manually to NA and assigned proper permissions before they can be authenticated via TACACS+. Once a user is identified as a TACACS+ user in NA, you cannot remove this designation.

RADIUS Authentication

RADIUS (Remote Authentication Dial-In User Service) enables:

- A network access server to operate as a RADIUS client. The RADIUS client is responsible for passing information to designated RADIUS servers and then acting on the returned responses.
- RADIUS servers to receive connection requests, authenticate users, and then return all necessary client configuration information for proper connection.
- RADIUS servers to act as a proxy client to other RADIUS servers or others authenticating servers.

Note: RADIUS is not used for authorization/permissions. This means that the user must be added manually to NA and assigned proper permissions before they can be authenticated via RADIUS. Once a user is identified as a RADIUS user in NA, you cannot remove this designation.

To enable TACAC+ or RADIUS authentication, On the menu bar under Admin, select Administrative Settings and click the User Authentication tab. The User Authentication page opens. Be sure to click Save when you are done.

HP Server Automation (HP SA)

The HP Server Automation option enables the NA system to use the HP SA system for user authentication. As a result, HP SA users can use their HP SA credentials to login to NA. This option also enables you to display HP SA servers in network diagrams and link to HP SA servers from MAC Addresses. Refer to “NA/SA Integration” on page 198 for information.

HP Operations Orchestration (HP OO)

IT organizations often perform troubleshooting tasks manually using out-of-date troubleshooting guides that provide no audit trail of the actions being performed. Even when IT organizations deploy scripts as their automation solution, the scripts are hard to maintain and do not provide an audit trail.

The HP OO option enables you to launch HP OO flows in guided mode directly from the NA Web UI. To run unattended HP OO flows, you must create a command script for the language “Flow”. For information on launching unattended flows, refer to “HP Operations Orchestration (HP OO) Flows” on page 576 for information.

In general, the HP OO enables you to centralize all of your routine triage, troubleshooting, and maintenance tasks within NA. You can define which HP OO flows are available and then launch:

- An unattended HP OO flow to collect and present data from a 3rd party system given either one or multiple device IP addresses. Refer to “HP Operations Orchestration (HP OO) Flows” on page 576 for information.
- A pre-defined Manage Software Upgrade flow. This HP OO flow removes the router from monitoring systems, removes the router from the OSPF mesh, upgrades the IOS image, and then re-inserts the device into the OSPF mesh and re-adds it to the monitoring system. Refer to “Edit Menu Options” on page 232 for information on the Process Automation option.

For detailed information on HP OO, refer to the *HP Operation Orchestration User’s Guide* and the *HP Operation Orchestration Software Development Kit Guide*.

User Authentication Page Fields

Field	Description/Action
User Password Security	
Minimum User Password Length	Enter the minimum number of characters a password must contain. Passwords of less than this number of characters are considered invalid.
User Password Must Contain Upper and Lower Case	If checked, users must choose passwords that contain both lower-case and upper-case alphabetic characters.
Additional User Password Restriction	Select one the following options: • No additional restrictions (the default) • Must contain at least one non-alphabetic digit or special character • Must contain both at least one digit and at least one special character
Maximum Consecutive Login Failures	Enter the maximum number of allowed consecutive user authentication failures, after which the user will be disabled. A value of 0 (zero) indicates that this check should be skipped. (**Note**: This setting applies only to built-in user authentication and not to external authentication methods.)
External Authentication Type	
External Authentication Type	Select the type of external authentication you would like to use. Options include: • None (Local Auth) • HP Server Automation • HP Server Automation & TACACS+ • TACACS+ • RADIUS • SecurID • LDAP If you select TACACS+ or RADIUS, it can be configured in the section below. If you select LDAP, click the LDAP Setup link. Refer to "LDAP External Authentication Setup" on page 82 for information. SecurID has no additional external authentication options.
TACACS+ / RADIUS Authentication	
Primary TACACS+ or RADIUS Server	Enter the host name or IP address of the primary TACACS+ or RADIUS server.
Secondary TACACS+ or RADIUS Server	Enter the host name or IP address of the secondary TACACS+ or RADIUS server. This field is optional.
TACACS+ or RADIUS Secret	Enter the shared secret for the NA host configured on the TACACS+ or RADIUS server. A TACACS+ or RADIUS secret is the key (password) that the TACACS+ or RADIUS client (NA) uses to encrypt communications with the TACACS+ or RADIUS server. The client and server must agree on the secret so the server can decrypt the communications.

Field	Description/Action
TACACS+ or RADIUS Authentication Method	Select one of the following authentication methods used to encrypt communications between NA and the TACACS+ or RADIUS server: • PAP (Password Authentication Protocol) • CHAP (Challenge Handshake Authentication Protocol) • MSCHAP (Microsoft Challenge Handshake Authentication Protocol) • ARAP (TACACS+ only) • ASCII (TACACS+ only)
Use RADIUS NAS-IP instead of default NAS-ID	Selecting this option sends the RADIUS NAS-IP field using the NA Core information, instead of the default NAS-Identifier field. It will send the first non loopback IP address it finds for the NA Core. (**Note**: 'NAS' in this settings is not from the NA product. It is specific to RADIUS authentication.)
Fixed RADIUS NAS-IP string	Enter a constant string to use as the RADIUS NAS-IP field instead of the default IP Address found. This option can be used to tell NA what IP address to use for the NAS-IP field, rather than letting NA use its default. This should only be necessary for multiple network interface card system or to set the field to an IP address not bound to the server. (**Note**: 'NAS' in this settings is not from the NA product. It is specific to RADIUS authentication.)
HP Server Automation Authentication	
Twist Server	Enter the host name or IP address of the HP Twist server. Refer to the *HP Server Automation User's Guide* for information.
Twist Port Number	Enter the Twist port number (typically 1032) to connect to the HP Twist server. Refer to the *HP Server Automation User's Guide* for information.
Twist Username	Enter the Twist Web-services API (wsapi) username, typically *wsapiReadUser*.
Twist Password	Enter the Twist Web-services API (wsapi) password.
OCC Server	Enter the HP Command Center (OCC) host name for linking to connected servers. The OCC server is the HP Server Automation (HP SA) Web UI client. NA can create hyperlinks to HP SA. As a result, you can jump from the NA Server page to the HP SA Server page. Refer to "Servers Page Fields" on page 224 for information.
Default User Group	Select the name of the user group to which you can add HP SA authenticated users from the drop-down menu. This group enables you to set default permissions for HP SA users. Refer to "NA/SA Integration" on page 198 for information.
HP Operations Orchestration Authentication	
HP OO Hostname	Enter the hostname or IP address of the HP OO server.
HP OO Port	Enter the HP OO port number to connect to the HP OO server.
HP OO Service	Select one of the following connection options to the HP OO service: • https:// • http:// The HP OO service uses SSL or plain text.

Field	Description/Action
HP OO Username	Enter the HP OO Username.
HP OO Password	Enter the HP OO password.
Guided Flow Names	Enter a guided flow name in the right-hand box and click Add Pattern <<. The flows applies to all device families. For example, if you prefix the guided flow name with *Cisco IOS:flow 1*, the guided flow applies to all devices that belong to the Cisco IOS device family. You can select a guided flow name in the left-hand box and then click Delete Pattern to delete the guided flow name. Refer to the *HP Operations Orchestration User’s Guide* for information on configuring flows. Refer to the “Edit Menu Options” on page 232 for information on logging into to HP OO.

LDAP External Authentication Setup

To enable LDAP external authentication:

1. On the menu bar under Admin, select Administrative Settings and click User Authentication. The Administrative Settings - User Authentication page opens.
2. Scroll down to the External Authentication Type field.
3. In the External Authentication Type field, select LDAP and click Save.
4. Click the LDAP Setup link. The LDAP Setup Wizard opens. If you have previously setup LDAP authentication, the following information is displayed:
   - LDAP Authentication Status
   - LDAP Authentication Server Host
   - Port number
   - Connection User Name
   - Connection user password
   - Search Base
   - If you using a secure connection
   - Server timeout

Note: NA checks that the fields are the same each time a user logs in. If necessary, NA updates the User field information with the corresponding information from LDAP. For example, if the NA administrator manually updates User A in NA and changes User A's Email address, the next time User A logs in, NA automatically changes User A's Email address to the value found in LDAP.

The following table guides you through the setup process.

Step	Action
1	At the Welcome to the LDAP Setup Wizard page, click Next. Enter the following information and click Next: • Server Type —Select the server type, either Active Directory (the default) or Generic LDAP. • Server Name — Enter the hostname of the LDAP or Active Directory server, i.e., the hostname or IP address of the AD/domain controller. • Port — Enter the LDAP request port number. Use port 389 or port 636 (for SSL) for a single domain configuration. • Connection Type — Select either Regular Connection (the default) or Secure Connection (SSL). Be sure to select Secure Connection when connecting to the directory server. (**Note**: If you enable this option and the certificate of your directory server/domain controller server is not signed by one of the recognized CAs, you must manually import the certificate to the server where NA is running.) For detailed information on LDAP SSL Configuration, refer to “LDAP SSL Configuration” on page 83. • Server Timeout — Enter the timeout, in milliseconds, for the LDAP operation. If an LDAP operation takes longer than this value, the operation will be aborted.

Step	Action
2	Enter the following information and click Next: • Connection User Name — Enter the connection user name. Keep in mind that to query user information from the AD server, NA should bind to the AD server with a domain user account (DN). The DN can be in the Windows 2000 LDAP format or in Windows 2000 User Principal Name (UPN) format. The Windows 2000 UPN format is a short-hand notation that uniquely identifies the DN in the LDAP tree. Both the user account and respective domain are included in the UPN. An example of a Windows 2000 UPN DN is *jsmith@hp.com*. • Connection User Password — Enter the connection user password • Search Base — Enter the search base. The search base is the starting point in the LDAP directory for LDAP searches. Ideally, the search base should be set to the root domain of the entire AD forest. This enables NA to query the entire Windows 2000 AD forest. If the search base is set at a particular OU level, only child objects of that particular OU can be queried. Similarly, if the search base is set at a particular domain level, only child objects of that particular domain can be queried. For this reason, the search base should be as general as possible.
3	Indicate which security groups can access NA. You can use the Find option to locate user groups in LDAP and click Next.
4	You can verify the External Authentication setup by entering the user name and passwords then click the Test Login button. Be sure to click the Save button to save the setup information. If there are no errors, the following message is displayed and the External Authentication Setup Summary page is updated: `Successfully updated External Authentication settings.`

LDAP SSL Configuration

For LDAP SSL configuration:

1. Install an Enterprise Certificate Authority on a Windows 2000 or Windows 2003 Server. All Domain Controllers in the forest will automatically enroll for and install the appropriate certificate.
2. Open the Default Domain Controller Policy using the Group Policy Editor.
3. Under Computer Configuration, click Windows Settings.
4. Click Security Settings, and then click Public Key Policies.
5. Click Automatic Certificate Request Settings.
6. Use the wizard to add a policy for Domain Controllers.

For more information, see the Microsoft Knowledge Base article Q247078.

For certificate importing:

1. Start the Certificate Authority management console (usually on the LDAP server) by clicking Start > Programs > Administrative Tools > Certification Authority.
2. Under Certificate Authority Local, find the Certificate Authority that issues certificates for your domain controllers.
3. Right-click the Certificate Authority and select Properties.
4. On the General tab, click View Certificate.

5. Select the Details tab and Copy to file.
6. Using the wizard, export the certificate to a Base64 Encoded file.
7. Copy this file to the NA server.
8. At a Windows command prompt, go to:
   `<install directory>\jre\bin`
9. Enter: keytool -import -file PATH_TO_THE_CERT_FILE -alias ADSCert -keystore ../../server/ext/jboss/server/default/conf/truecontrol.keystore

   The keystore password is “sentinel”.

   Replace the `PATH_TO_THE_CERT_FILE` with the absolute path of the file created in step 7.
10. Restart NA with the Services Applet (or /etc/init.d/truecontrol script on Solaris or Linux). If you restart NA from the UI, the keystore changes will not be loaded.

Server Monitoring

Server monitoring enables you to check on the overall health of the NA server. Alert notification and event logging are triggered when a error is discovered. All of the server monitors are pre-packaged and shipped with NA.

In the event that a monitor receives an error, a NA Monitor Error event is triggered and notification of the error is sent to the System Administrator. Keep in mind that the system will not continue to send Monitor Error events for that monitor when it is checked later and is still in an error state. Once a monitor is in an error state, and an event to that effect is triggered, the system will only send a Monitor Okay event if the state changes to okay.

Note: If the system is restarted and the error condition persists, a new Monitor Error event is triggered. If the database is inaccessible, the system will attempt to email that fact to the administrator.

The Server Monitoring page enables you to configure server monitors. You also have the option of enabling all or only specific server monitors. The results of the most recent monitor runs are stored in the Monitor log file and can be viewed in the System Status page. Refer to "Server Monitoring Page Fields" on page 85 for information on the System Status page.

Note: Only Administrators have permission to change monitoring tasks settings. All users can view monitoring results.

To view the Server Monitoring page, on the menu bar under Admin, select Administrative Settings and click Server Monitoring. The Server Monitoring page opens.

Server Monitoring Page Fields

Field	Description/Action
Server Monitoring	
Enable Server Monitoring	If checked (the default), server monitoring is enabled. Email notification in the event of an NA error is generated. The most recent results are stored in the Monitor log file and can be viewed from the System Status page. If not checked, the scheduled monitor check will no longer be executed. However, server monitors can still be run manually.
Delay on Startup Before Starting Monitoring	Enter the number of minutes to delay starting server monitoring after startup. The default is two minutes.
Delay Between Monitoring Runs	Enter the number of minutes to delay between monitoring runs. The default is 360 minutes.
Enable the ConfigMonitor	If checked, the Config monitor is enabled. This monitor checks that the installed .rcx files and other configuration files are okay. This monitor makes a backup of the initial installed .rcx files and keeps a backup of the latest error-free installed .rcx files.

Field	Description/Action
Enable the DatabaseDataMonitor	If checked, the Database Data monitor is enabled. This monitor checks that all critical system components are in the database, for example that an admin user exists, that there is only one crypto key, that one paused or pending Inventory snapshot task exists, and so on. This monitor makes a backup of the crypto key and the admin email address (for use if the database server is down).
Enable the DatabaseMonitor	If checked, the Database monitor is enabled. This monitor checks for database connectivity, for example if there are invalid credentials or too many connections.
Enable the DiskMonitor	If checked, the Disk monitor is enabled. This monitor checks for low disk space conditions.
Enable the DynamicDeviceGroup Monitor	If checked, the DynamicDeviceGroup monitor is enabled. This monitor counts the number of dynamic device groups.
Enable the FTPMonitor	If checked, the FTP monitor is enabled. This monitor sends a FTP file with a timestamp to the local machine, and then checks the file system to verify it was written correctly.
Enable the HTTPMonitor	If checked, the HTTP monitor is enabled. This monitor ensures that the NA Web server is running correctly.
Enable the LDAPMonitor	If checked, the LDAP monitor is enabled. This monitor checks that the LDAP server is available.
Enable the LicenseMonitor	If checked, the LicenseMonitor is enabled. This monitor checks if the available licenses drop below the percentage of managed devices and/or if the next license to expire is within the number of days specified. Refer to the "Monitor Configuration" section below for more information.
Enable the LogMonitor	If checked, the LogMonitor is enabled. The LogMonitor is responsible for managing log settings. When log levels are left at Trace or Debug for too long, system performance can suffer. The LogMonitor routinely checks for logs left at these lower levels and resets them to Error.
Enable the MemoryMonitor	If checked, the Memory monitor is enabled. This monitor checks for low memory conditions.
Enable the RMIMonitor	If checked, the RMI monitor is enabled. This monitor checks that RMI access to the NA EJBs is working. It ensures that some other EJB container (Java application server) has not grabbed the RMI port.
Enable the RunExternalTaskMonitor	If checked, the Run External Task monitor is enabled. This monitor ensures the NA server can run an external .bat or .sh file.
Enable the SatelliteMonitor	If checked, the Satellite monitor is enabled. This monitor checks that Syslog and TFTP are running and that the Satellite is the same version as the NA Core. For information on NA Satellite configuration, see the *NA Satellite Guide*.
Enable the SMTPMonitor	If checked, the SMTP monitor is enabled. This monitor makes a Telnet connection to Port 23 on the configured mail server, sends a SMTP *QUIT* command, and waits for the proper *221* response code.

Field	Description/Action
Enable the SSHMonitor	If checked, the SSH monitor is enabled. This monitor tests the connection to the SSH server embedded in NA.
Enable the SoftwareImage Management Monitor	If checked, the SoftwareImanageManagement monitor is enabled. If SWIM is enabled, this monitor checks that it can communicate with the SWIM server.
Enable the SyslogMonitor	If checked, the Syslog monitor is enabled. This monitor sends a Syslog message to NA and ensures that it is received by the NA Management Engine.
Enable the TelnetMonitor	If checked, the Telnet monitor is enabled. This monitor checks that the Telnet server embedded in NA is running correctly.
Enable the TFTPMonitor	If checked, the TFTP monitor is enabled. This monitor sends a TFTP file with a timestamp to the local machine, and then checks the file system to verify it was written correctly.
Monitor Configuration	
Check the Inventory Snapshot in the DatabaseDataMonitor	If checked, the Inventory snapshot in the Database Data monitor is checked.
Warning Threshold for Free Disk Space	Enter the threshold to trigger the free disk space warning message. The default is 20 MB.
Error Threshold for Free Disk Space	Enter the threshold to trigger the free disk space error message. The default is 10 MB.
Drives To Monitor for Disk Space	Enter a drive in the right-hand box and then click Add Drive <<. To delete a drive, select the drive in the left-hand box and click Delete Drive.
Warning Threshold for Managed Devices Count	Enter a percentage of your total licenses. If the available licenses drop below this percentage, a warning is issued. Device count threshold defaults to 10%.
Warning Threshold for License Expiration	Enter a number of days. If the next license expires within the number of days specified, a warning is issued. The expiration date threshold defaults to 30 days.
Automatically reset logs to ERROR and close task logs when log monitor detects an issue.	This option is checked by default. When this option is checked, if the log monitor detects that a log has been set to too low a level for too long, it will automatically reset that log's level to ERROR.
Time that logs set to set TRACE level will not be reported as open too long.	The default is 48 hours. The time a log can be at TRACE level without the log monitor detecting it has been set too low for too long.
Time that logs set to set DEBUG level will not be reported as open too long.	The default is 48 hours. The time a log can be at DEBUG level without the log monitor detecting it has been set too low for too long.
Time that active task logs will not be reported as open too long.	The default is six hours. The time that active task logs will not be reported as open too long.

Field	Description/Action
Warning Threshold for Free RAM	Enter the threshold to trigger the Free RAM warning message. The default is 20 MB
Error Threshold for Free RAM	Enter the threshold to trigger the Free RAM error message. The default is 10 MB.
Delay for SSH Thread Check	Enter the delay for the SSH Thread check. The default is 15000 milliseconds.
Delay for TFTP File Check	Enter the delay for the TFTP file check. The default is 5000 milliseconds.
Delay for FTP File Check	Enter the delay for the FTP file check. The default is 5000 milliseconds.
Delay for Syslog message to show up	Enter the delay for the Syslog message to be displayed. The default is 45000 milliseconds.

Be sure to click Save to save your changes.

3rd Party Integrations

Integrating with HP Network Node Manager i Software (NNMi) provides the following features and benefits in a system already running both NNMi and NA:

- Alarm integration
- Access to NA configuration history from NNMi
- Operations efficiency

To enable the HP NNMi–HP NA integration, follow the procedure in the *HP Network Node Manager i Software—HP Network Automation Integration Guide*. This procedure includes configuring communication between NA and NNMi on the HP NNMi–HP NA Integration Configuration form in the NNMi console. The integration sets the corresponding fields on the 3rd Party Integrations page in the NA console.

To change the behavior of the HP NNMi–HP NA integration for NNMi device rediscovery triggers, out-of-service triggers, and SNMP community string propagation, update the configuration on the 3rd Party Integrations page in the NA console.

Note: You cannot enable or disable the NA-NNMi integration from this page in the NA console. Use this page only to change the integration behavior for NNMi device rediscovery triggers, out-of-service triggers, and SNMP community string propagation.

For detailed information about the HP NNMi–HP NA integration, see the *HP Network Node Manager i Software—HP Network Automation Integration Guide*.

To view the 3rd Party Integrations page, on the menu bar under Admin, select Administrative Settings and click 3rd Party Integrations. The 3rd Party Integrations page opens.

3rd Party Integrations Page Fields

Field	Description/Action
3rd Party Integrations	
3rd Party Integrations	Select one of the following options: • Enabled • Disabled (the default) You do not need to change this setting. Note the following: • Enabling the HP NNMi–HP NA integration from the NNMi console sets this field to Enabled. • Setting this field to Disabled does not disable the HP NNMi–HP NA integration.
NNMi Integration	
NA User	Enter the NA-NNMi integration user name.
NA Partition	Enter the NA-NNMi integration partition name. Refer to “Partitions” on page 158 for information on creating NA partitions.

Field	Description/Action
NNMi Host	Enter a NNMi server host name or IP address.
NNMi Protocol	Select the protocol for connecting to the NNMi web services.
NNMi Port	Enter the web services port number on the NNMi management server. For HTTP connections, the default port is 80. For HTTPS connections, the default port is 443.
NNMi User	Enter a NNMi login user name.
NNMi Password	Enter a NNMi login password.
Rediscover Hosts After Tasks	Select tasks from the list. The selected tasks will cause NNMi to rediscover the device if the task ran successfully. The default tasks are: • Update Device Software • Deploy Passwords • Reboot Device • Discover Driver
Out of Service Events	Select tasks from the list. When the tasks start, NA calls the NNMi Web service to designate the device as “Out of Service.” As a result, NNMi temporarily no longer manages the device. After the task is finished, NA calls the NNMi Web service and designates the device as managed. The default tasks are: • Update Device Software • Deploy Passwords • Reboot Device
If the device task fails	Select one of the following options: • Sets the device back in service (the default). • Does not set the device back in service.
If the device compliance check fails after the task completes	Select one of the following options: • Sets the device back in service (the default). • Does not set the device back in service.
Propagate SNMP Community Strings	Select one of the following options: • Enabled • Disabled (the default)

Viewing Monitor Results

The System Status page displays the results of the most recent monitor runs. To view the System Status page, on the menu bar under Admin, click System Status. The System Status page opens.

System Status Page Fields

Field	Description/Action
Run All link	Run all of the listed monitors.
Configure Server Monitoring link	Opens the Server Monitoring Page. Refer to "Server Monitoring Page Fields" on page 85 for information.
Monitor Name	Displays the monitor name. Each monitor can return a variety of messages about the subsystem it is monitoring. Refer to "Monitor Messages" on page 92.
Status	Displays the monitor status, including: • Okay • Warning • Error • Disabled
Last Checked	Displays the date and time the monitor was last run.
Result	Displays information about the results.
Actions	You can select the following options: • Run Now — Runs the monitor immediately. • View Details — Opens the Monitor Details page, where you can view details about the monitor, including a description of the monitor, the status, results, and additional diagnostic information. • Start/Stop Service — Opens the Start/Stop Services page. Refer to "Starting and Stopping Services" on page 96 for information.

Monitor Messages

Each monitor can return a variety of messages about the subsystem it is monitoring. This section details some of these messages and possible corrective actions.

Monitor	Description/Resolution
BaseServerMonitor	<threadname> is not running. — A thread necessary for proper functioning of NA has failed for an unknown reason. You may have to restart the NA management engine.
ConfigMonitor	• Missing file <filename>.rcx — One of NA's required configuration files is missing. Contact Support for assistance. • Error getting required config from <filename>.rcx — One of NA's configuration files has become corrupted. Contact Support for assistance. • Exception parsing rcx file: <filename> — One of NA's configuration files has become corrupted. Contact Support for assistance.
DatabaseMonitor on MySQL	• Cannot connect to the MySQL server on <servername>:3306. — There is no MySQL server running at the location where NA is trying to connect. You can either restart the MySQL service or verify that the NA connection information is correct. • Communication link failure: java.io.IOException — The connection to the MySQL server has been lost. You may have to restart the NA management engine or restart the MySQL service. • Access denied for user: <username> to database <database_name> — NA is trying to connect to the wrong database or there is some permission problem with the existing database. Verify that the NA connection information is correct. • Invalid authorization specification: Access denied for user: <username> (Using password: YES) — NA is trying to connect using the wrong username or password. Reset the NA database username and password to the correct values. • General error: Table NA.RN_CRYPTO_KEY doesn't exist — NA can connect to the database using the credentials given, but the database is either not a NA database or is corrupt (as it is missing the RN_CRYPTO_KEY table). Verify that the NA connection information is correct.
DatabaseMonitor on Oracle	• Error establishing socket. Connection refused: connect — There is no Oracle server running at the location where NA is trying to connect. You may have to restart the Oracle service or verify that the NA connection information is correct. • Connection reset by peer: socket write error. — The connection to the Oracle server has been lost. You may have to restart the NA management engine or restart Oracle. • ORA-12505 Connection refused, the specified SID (<database_name>) was not recognized by the Oracle server. — NA is trying to connect to the wrong database name. Verify that the NA connection information is correct. • ORA-01017: invalid username/password; logon denied — NA is trying to connect using the wrong username or password. Reset the NA database username and password to the correct values. • ORA-00942: table or view does not exist — NA can connect to the database using the credentials given, but the database is either not a NA database or is corrupt (as it is missing the RN_CRYPTO_KEY table). Verify that the NA connection information is correct.

Monitor	Description/Resolution
DatabaseMonitor on SQLServer	• Error establishing socket. — There is no SQLServer running at the location where NA is trying to connect. Either restart the SQLServer service or verify that the NA connection information is correct. • Connection reset by peer: socket write error — The connection to SQLServer has been lost. Either restart the NA management engine or restart SQLServer. • Cannot open database requested in login <database_name>. Login fails. — NA is trying to connect to the wrong database name or there is some permission problem with the existing database. Verify that the NA connection information is correct. • Login failed for user <username>. — NA is trying to connect using the wrong username or password. Reset the NA database username and password to the correct values. • Invalid object name RN_CRYPTO_KEY. — NA can connect to the database using the credentials given, but the database is either not a NA database or is corrupt (as it is missing the RN_CRYPTO_KEY table). Verify that the NA connection information is correct.
DatabaseData Monitor	• Could not find an administrative user. — NA does not have an administrative user configured. Contact Support for assistance. • Multiple crypto keys exist. — NA contains multiple crypto keys in its database. Contact Support for assistance. • Current key does not match saved key. — NA is now using a different crypto key. Contact Support for assistance. • More than one crypto key. — NA is now using a different crypto key. Contact Support for assistance. • Could not find an Inventory group snapshot. — NA does not contain a task to collect configs from all of the devices in the system. Create a Snapshot task for the Inventory group. • Could not find a reporting task. — NA does not contain a task to generate summary reports. Create a Generate Summary Reports task. • Could not find a pruner task. — NA does not contain a task to prune old data from the database. Create a Prune Database task.
DiskMonitor	Disk/Filesystem <filesystem> has only <space> bytes free. Error threshold is <limit> bytes. — The NA server is close to filling up a disk drive. Delete unnecessary files from the disk drive.
HTTPMonitor	Did not get NA login page. — An application is running on the configured HTTP/HTTPS port, but it does not appear to be the NA web server. Stop any other web servers (e.g. IIS) running on the NA server and then restart the NA management engine.

Monitor	Description/Resolution
LDAPMonitor	• ActiveDirectory is not in use. — This is an informational message that reveals the NA server is not configured to use LDAP. • Exception in LDAPMonitor: javax.naming. CommunicationException: <hostname>:389 — The host <hostname> does not exist. Correct the Server Name setting for external authentication. • Exception in LDAPMonitor: javax.naming. CommunicationException: <hostname>:389 — The host <hostname> exists but is not accepting connections on the LDAP port (389). Check that the Server Name setting is correct. If so, check that the LDAP server is running on that host. • Exception in LDAPMonitor: javax.naming.AuthenticationException — The Connection User Name or Connection User Password setting for external authentication is incorrect. Check that these settings are correct.
LicenseMonitor	Warnings such as “License about to expire” or “Device count exceeds the current threshold of available licenses” are displayed in the Results column. If no warnings are displayed, the number of available device licenses is displayed, for example, “3454 of 3600 device licenses remaining.” Click the View Details link to view details about the license, such as used and free licenses, and the license expiration date. (**Note**: If multiple licenses are used, the expiration date is the date of the next license to expire.)
MemoryMonitor	<bytes> bytes free. — This is how much memory is available to the system. It is approaching an insufficient amount for proper system functioning when an Error condition occurs. Contact Support for assistance.
RMIMonitor	Could not connect to RMI port 1099. — Another application is using the port 1099 that NA needs for its client and API to function properly. Stop the application that is using port 1099 and restart the NA management engine. If this is not possible, contact Support for assistance.
RunExternalTask Monitor	• CreateProcess: <path>\tc_test.bat error=5 — NA does not have permissions to access the test script (and possible other scripts). Check the file system permissions for NA’s directories. • CreateProcess: <path>\tc_test.bat error=2 — NA cannot find the test script. Contact Support for assistance. • Running <path>\tc_test.bat from directory <path> Got result code: 0 Got output: <text> — The test script is corrupted. Contact Support for assistance.
SMTPMonitor	• SMTP Server name is blank. — The SMTP Server name administrative setting in NA is blank. Verify that a mailserver is set in the Administrative Settings page. • Can't open Telnet connection to <hostname> 25 — Either NA cannot connect to <hostname> or the host is not receiving connections on the SMTP port (25). Verify that the correct mailserver is set in the Administrative Settings page. Verify that the NA server can access port 25 on that server. • Timeout waiting Expected: 220 Received. — An application is running on port 23 on the configured mail server, but it does not appear to be an SMTP application since it is not responding with the proper SMTP codes. Verify that the correct mailserver is set in the Administrative Settings page.
SSHMonitor	Unknown problem connecting to SSH server. — The NA SSH server is not working correctly. Make sure no other application is listening to the SSH port that NA is using. Restart the NA management engine.

Monitor	Description/Resolution
SyslogMonitor	Test syslog message did not get processed. — NA's built-in Syslog server is either not running or has some problem. Contact Support for assistance.
TelnetMonitor	• Can't open Telnet connection to <hostname> 23. — The NA Telnet server is not working correctly. Restart the NA management engine. If this does not correct the problem, contact Support for assistance. • Timeout waiting Expected: HP Login: Received. — An application is running on the configured Telnet port, but it does not appear to be the NA Telnet server. Modify the NA Telnet server listening port.
FTPMonitor	• Connection timed out to the FTP server. — The FTP server is either not running or not accepting connections. Restart the FTP server. • Test FTP file was written but could not be read successfully. Check FTP path setting. — The FTP file was successfully written to the FTP server, but could not subsequently be read from the filesystem. Check that the FTP path setting is correct in the NA management engine. • Found checkpoint file but timestamp is out of date. — The most recent file write attempt failed, and the system found a previous checkpoint attempt. This means that the FTP server worked at some point in the past but is not working now. Restart the FTP server.
TFTPMonitor	• Connection timed out to the TFTP server. — The TFTP server is either not running or not accepting connections. Restart the TFTP server. • Test TFTP file was written but could not be read successfully. Check TFTP path setting. — The TFTP file was successfully written to the TFTP server, but could not subsequently be read from the filesystem. Check that the TFTP path setting is correct in the NA management engine. • Found checkpoint file but timestamp is out of date. — The most recent file write attempt failed, and the system found a previous checkpoint attempt. This means that the TFTP server worked at some point in the past but is not working now. Restart the TFTP server.

Starting and Stopping Services

These are the four primary functional units within NA, including:

- NA Management Engine
- HP Live Network
- TFTP, FTP, and Syslog servers
- Software Image Management server

Typically, you would only stop, start, or restart a service when working with Customer Support.

To start/stop services or reload drivers, on the menu bar under Admin, click Start/Stop Services. The Start/Stop Services page opens.

Note: When using the Web user interface to start and stop NA services, you could lose the ability to navigate to the previous page. If you click the Back button, you could see a page with the text: null. Click your browser's Back button instead.

Start/Stop Services Page Fields

Field	Description/Action
Management Engine	Select one of the following options: • Stop — Stops the Management Engine (also referred to as the NA server). This is the main service within NA. • Restart — Restarts the Management Engine.
HP Live Network	Select one of the following options: • Reload Drivers — Enables you to reload NA drivers so that they are available when adding new devices. The Reload button does not discover drivers. • Reload Content — Content is a suite of NA enhancements and extensions available from HP which do not require a product upgrade. However, a subscription to some content service(s) may be required. For example, NA supports content import of software level policies via the HP Security Service. As part of the HP Security Service, you can download software level policies from HP to assist you in managing network integrity. Refer to "Software Levels Page Fields" on page 437 for more information.
TFTP Server	Select one of the following options: • Start — Starts the TFTP server. NA uses this primarily to retrieve and deploy configurations. (**Note**: TFTP provides the best performance. If TFTP is not available, NA uses Telnet or SSH to process configurations.) • Stop — Stops the TFTP server. • Restart — Restarts the TFTP server.

Field	Description/Action
FTP Server	Select one of the following options: • Start — Starts the FTP server. NA uses this primarily to retrieve and deploy configurations. (**Note**: If FTP is not available, NA uses TFTP, Telnet, or SSH to process configurations.) • Stop — Stops the FTP server. • Restart — Restarts the FTP server.
Syslog Server	Select one of the following options: • Start — Starts the Syslog server. NA could be your only Syslog server, or other Syslog servers may forward messages to NA. NA uses Syslog messages to detect real-time change events and attribute them to users. • Stop — Stops the Syslog server. • Restart — Restarts the Syslog server.
Software Image Management Server	Select one of the following options: • Start — Starts the Software Image Management server. The Software Image Management server provides software images that are available from Cisco.com, along with preferred recommendations. For information on the Device Software Image Recommendation page, refer to "Device Software Image Recommendation Page Fields" on page 225. • Stop — Stops the Software Image Management server. • Restart — Restarts the Software Image Management server.

Logging

Logging is the means of obtaining information about what NA is doing when performing its functions. In the case of system failures, logging is the primary means of identifying what is going wrong and the means of troubleshooting the issue.

Log Levels

Logs are provided in the form of a series of messages that record events occurring in the system. By default, these messages only record significant events, such as errors, unexpected situations, or cases of potentially bad data. This is termed the ERROR logging level. Logging levels are a means of indicating how much information is recorded about an aspect of the system. The lower the level, the more messages recorded.

NA Log levels include:

- FATAL — Messages are only recorded in cases where fatal errors are encountered. This is the highest logging level.
- ERROR — Messages are recorded primarily to show error cases. This is the default logging level.
- DEBUG — Messages are recorded to help identify why a particular error has occurred. This is the middle logging level.
- TRACE — Messages are recorded about the general functioning of the system. This is the lowest logging level.

Note: Setting to many logs can significantly degrade system performance. In most cases you should only adjust logging levels when instructed to do so by Customer Support.

Log Names

Logs are given names that provide some idea of what part of the system they relate to. Log names are hierarchical, meaning that one log can include a number of sub-logs. NA provides the following top-level logs:

- API — Logging related to interaction with NA through means other than the standard Web interface.
- Cache Provider — Logging related to tracking database caching performance improvements.
- DDK — Logging related to the DDK.
- Device — Logging related primarily to interaction with devices.
- External — Logging related to external utilities, such as TFTP, FTP, Syslog server, and connectors to third-party applications.
- Feature — Logging related to specific NA features.
- FlexUI — Logging related to tracking issues specific to the Flex user interface components (for example, the Device Selector).
- System — Logging related to internal functioning of the NA system and server.
- Web UI — Logging related to interaction with NA through its Web interface.

There are many sub-logs under each of these broad categories. For example, under the Device log there are the Access, Session, and Data sub-logs. These sub-logs include more specialized logging focused on access to devices, interaction with them, and the data retrieved, respectively. Each of these sub-logs has sub-logs of its own for further specialized focus when needed.

Sub-logs are referenced by preceding them with the containing log name followed by a slash, for example:

- Device
- Device/Access
- Device/Access/AuthenticationRules
- Device/Session
- Device/Session/SSH
- Device/Session/SNMP

The level of any log is equal to the lowest level set for that log or any of its containing logs. As a result, if the Device/Session/SNMP log was set to the ERROR level, but the Device/Session log was set to the DEBUG level, the Device/Session/SNMP log would be treated as if it, too, was set to the DEBUG level.

Since enabling a large number of logs at a low level can degrade system performance, you should be careful in setting a broad container log to a low level since this automatically sets all of its contained logs to that level as well.

Note: Although log names provide some clue as to the part of the system they relate to, you should always contact Customer Support for instructions before manipulating log settings.

Session Logs

Session Logs are a special type of log used to show how NA interacts with a device during a task. This is only available for those tasks that actually interact with devices. The output of this log is automatically inserted into the task results.

Session logs are enabled via a checkbox provided in each device-specific task creation page. In most cases, re-running a task will automatically result in the session log being enabled even if it was not enabled when the task was first run. Refer to "Chapter 7: Scheduling Tasks" on page 277 for task creation information.

Session logs are intended to help identify issues that arise due to common device interaction problems, such as connectivity failures, authentication failures, or scripting errors. They can also be used to show what NA is doing to achieve a certain result on the device, and confirm that it is, in fact, doing the right thing.

The session log shows information about:

- Task process steps (This information is specific to NA. It is used to help organize the log.)
- Connection attempts via various protocols
- Disconnections and connection failures
- The commands sent to the device
- The results received from the device
- The results that were expected from the device (if any)

Note: Many failure cases will result from a command being sent with a certain result expected. When the device responds with a different result, the task fails.

When reviewing Session Logs, keep in mind that NA attempts to complete a task by any means possible. Therefore, you could see failures in the Session Log even if a task completes successfully. For example, a configuration snapshot could succeed despite the session log showing failed TFTP upload attempts. These failed attempts could indicate a problem with TFTP connectivity to the device, but the failure only causes NA to try another means to obtain the configuration. If these other means succeed, the task will succeed in spite of the TFTP failures.

Task Logs

Task Logs are general-purpose logs created to track system activity related to one specific task. Task logging is limited to tasks that are run once (not on a recurring schedule). In addition, if the task is device-related, the Task Log is only available when run against a single device. Not all types of tasks in NA support Task Logs. For example, Task Logs are not available when you create a new event notification and response rule for a task.

Note: Although all NA users can create a task-specific log, only users with Administrative privileges can view and download them. If you do not have the proper privileges to view and download logs, contact your NA system administrator, and if necessary have him or her provide the log information to Support.

If task logging is available for a task, a Task Logging section is provided in the task creation page. If the task being created is not appropriate to task logging (because it is being run against a group of devices or on a recurring schedule, for example), the task logging interface will be unresponsive.

Enabling task logging for a task consists of enabling the checkbox and choosing one or more log names. A list of all available log names are provided. This list could include an entry for a default set of logs appropriate to the task you are creating. You can select as many logs as you like, including or excluding the default set. Log names that are selected from the list are automatically set to TRACE level for the Task Log.

When you run the task, a log specific to that task is generated as a file and stored along with the NA server logs. If, for any reason, the task log file is unable to be created, the task will immediately fail with an error message. No information about the task log is provided in the task results page.

Server Logs

Server Logs are the logs for the entire NA system. They contain messages recording the activity of all tasks and all other processes in one location. Server Logs are enabled in the Troubleshooting page. Refer to “Troubleshooting Page Fields” on page 102 for information.

Note: Server logs should only be used as instructed by Customer Support.

Log Management

In addition to enabling and disabling the different types of logs, NA can manage how long log files are retained and provide performance management techniques to reset log levels after a period of time. Refer to “Server Page Fields” on page 54 for details on managing how long log files are retained. Refer to “Server Monitoring” on page 85 for performance management techniques on how NA automatically resets log levels and how you can modify the setting.

Troubleshooting Page Fields

To view the Troubleshooting page, on the menu bar under Admin click Troubleshooting. The Troubleshooting page opens.

Field	Description/Action
Send Troubleshooting Information link	Opens the Send Troubleshooting Info page, where you can compose an email and send system information and logs to Customer Support. Refer to "Send Troubleshooting Page Fields" on page 31 for information.
Download Troubleshooting Information link	Enables you to download troubleshooting information. Refer to "Send Troubleshooting Page Fields" on page 31 for information.
Send Test Email to Admin User link	Sends an email to the System Administrator. It is used to ensure that NA's email system is configured correctly and to troubleshoot cases where email (in particular troubleshooting email) is not getting through.
Enable logging for	Select one or more components for which you want to enable logging. Refer to "Logging" on page 98 for detailed information about Logging.
and for	Enter any additional software components that are not on the list.
at level < > and above	Select a logging level. Options include: • Fatal (fewest messages) • Error (default) • Debug • Trace (most messages) Refer to "Log Levels" on page 98 for detailed information.
Keep < > days worth of logs	Enter how long you would like to keep log data. The default is two days. (**Note**: Log data can require large amounts of disk space.)
Reset	If checked, all logs are reset to the default logging level (Error) when you click the Submit button.

Reviewing Drivers

The Drivers page displays a list of the installed drivers on your system and the number of drivers currently in use. The Drivers page enables you to determine which NA drivers were built in-house or endorsed by HP, and as a result are supported by HP.

To view the Drivers page, on the menu bar under Admin click Drivers. The Drivers page opens.

Drivers Page Fields

Field	Description/Action
Reload Drivers link	Enables you to reload drivers when you have added, removed, or updated drivers for NA.
Description	Displays the driver name.
Internal Name	Displays the unique driver name used to identify the driver. This is used by Support.
Package Name	Displays the driver package name.
Version	Displays the driver version.
Build Number	Displays the current NA build number.
Author	Displays the name of the person who wrote the driver. If not specified, it implies that the driver was built in-house by HP.
Certified	Displays if the driver is certified. A certified driver is a NA driver either created by HP, or created by third party and endorsed by HP.
In Use	Displays if the driver is currently in use.

Chapter 3: Adding Devices and Device Groups

Use the following table to quickly locate information.

Topic	Refer to:
Getting Started	"Getting Started" on page 106
Adding Devices	"Adding Devices" on page 108
Editing Devices	"Edit Device Page Fields" on page 113
Bare Metal Provisioning	"Bare Metal Provisioning" on page 118
Adding New Device Templates	"Adding New Device Templates" on page 124
Using the Add Device Wizard	"Using the New Device Wizard" on page 127
Importing Devices	"Importing Devices" on page 128
Creating Device Password Rules	"Creating Device Password Rules" on page 134
Adding Device Groups	"Adding Device Groups" on page 138
Dynamic Groups	"Dynamic Device Groups" on page 142
Device Selector	"Device Selector" on page 144
Viewing Device Groups	"Viewing Device Groups" on page 146
Segmenting Devices and Users	"Segmenting Devices and Users" on page 150
Setting Up The HP Gateway	"Setting Up The HP Gateway" on page 154
Editing Device Groups	"Editing Device Groups" on page 162
Editing a Batch of Devices	"Editing a Batch of Devices" on page 163
Discovering Device Drivers	"Discovering Device Drivers" on page 165
Listing Telnet/SSH Session	"Listing Telnet/SSH Sessions" on page 168
Using a Bastion Host	"Using a Bastion Host" on page 171

Getting Started

When you add a device, HP Network Automation Software (NA):

1. Auto-detects and assigns the correct device driver to enable communication with the device. This process is called Driver Discovery.
2. Takes a snapshot of the device to collect the system information and initial configuration.
3. Runs the set of core diagnostics, such as “NA Interfaces” and “NA Routing Table”. (Refer to “View Menu Options” on page 203 for a complete list of diagnostics.)

To successfully discover and snapshot a device, NA requires full access to the device, and may also require SNMP read access to the device.

Keep in mind that console servers are used to provide access to devices that are not currently reachable on the IP network, and may only be reachable via a serial connection over the device’s console port, for example devices with either a hardware failure, located in protected networks, or that do not run the IP protocol (IPX, ATM, and so on).

If you want to use a standard console server, for example a Cisco AS5xxx, that uses SSH authentication, you can connect from the console server to the target device by Telneting to the console server loopback address with the appropriate port number. To do this, you must:

- Configure the desired device(s) to use the SSH connection method.
- Configure the desired devices to use bastion host access. Be sure to provide the address and credentials for the console server as the bastion host.
- Set the device to use device-specific credentials (since in this case each device will have a different target port).
- Configure the appropriate access variables on each affected device. These variables might include:
  - hop_prompt = > (The Cisco console server prompt.)
  - hop_target_connect_protocol = telnet (Use Telnet to connect from console server to target device.)
  - hop_telnet_cmd_host = <loopback IP> (IP address of the loopback on the console server.)
  - hop_telnet_cmd_port = <device port> (Port number of the target device on the console server)

Note: Telnet Console servers with simple authentication, where the target device is still specified by port, can be supported using a set of Access Variable console_xxx. More complex Telnet console server configurations could require the use of customized bastion host access.

A bastion host is a host that has elevated privileges to access sections of a protected network that most other hosts cannot. This enables a management system to use a bastion host as a “hop” in managing elements on the protected network for which the bastion host has privileges. Typically, a bastion host is used for Internet and DMZ routers/switches, Extranet partners, and secured and/or private networks.

In both cases, NA uses console servers and bastion hosts as a means of accessing a device (usually via the CLI) to perform its normal management functions when other access methods, for example Telnet, SSH, FTP/TFTP, and SNMP, are not available.

Note: If all access methods are enabled, NA uses the following order to access devices: SSH, Telnet, SNMP, and Console. NA also performs file transfers before screen scrapes, for example: SSH+SCP, SSH+TFTP, SSH+Screen Scrape, Telnet+SCP, Telnet+TFTP, Telnet+Screen Scrape, SNMP+TFTP, and Console+Screen Scrape).

Device Groups Naming Convention

When referencing system generated device groups associated with policies, the device groups naming convention has been updated. For example, in previous releases, a device group named `DynamicCfgPolicyxxxx` (where `xxxx` is the name of the device group used for creating a group of devices for which to apply a policy), is now named `Config Policy Group - CONFIGPOLICYNAME - TIMESTAMP` (where `CONFIGPOLICYNAME` is the name of the configuration policy the device group was created from and `TIMESTAMP` is the time the device group was created.

Adding Devices

To add a new device, on the menu bar under Devices select New and click Device. The New Device page opens. When you are finished, you can either click the Save button or the Save And Add Another button.

Note: The Detect Network Devices task enables you to locate devices on your network that you want to place under NA management. Once you provide a range of IP addresses, NA scans your network looking for devices. Refer to "Detect Network Devices Task Page Fields" on page 343 for information.

New Device Page Fields

Field	Description/Action
Use Wizard link	Opens the Add Device Wizard. (**Note**: The Add Device Wizard opens automatically when no devices are present.) Refer to "Using the New Device Wizard" on page 127 for information on using the New Device Wizard.
IP Address (or DNS name)	Enter the device's IP address or DNS host name.
Hostname	Enter the device's host name, if applicable.
Site <name>	Select a Partition from the drop-down menu. This field is only displayed if you have configured one or more Security Partitions. In addition, the field name can be modified on the Partitions page. (Refer to "Partitions Page Fields" on page 158 for information.) In general, a Security Partition is a grouping of devices with unique IP addresses. Multiple Security Partitions can be managed by a single NA Core. A NA Core in an installation of a NA server, comprised of a single Management Engine, associated services, and a single database. **Note**: If a Security Partition applies to a Device/Device Group, there could be additional drop-down menus for each Security Partition. (Refer to "Segmenting Devices and Users" on page 150 for information on Security Partitions.)
Belongs to Groups	Displays the group(s) to which the device will be a member. Use the Device Selector to select groups. For information on how to use the Device Selector, refer to "Device Selector" on page 144.
Change Detection and Polling	Select one of the following options: • Enabled — When checked (the default), NA polls the device for changes as part of the regular polling task and when NA detects change events. • Polling Only — When checked, NA polls the device for changes as part of the regular polling task only. • Disabled — When checked, NA ignores change events related to the device. In addition, NA does not check the device for changes as part of the regular polling task. It a good idea to select this option during routine maintenance to exclude this device from the regular polling task.

Field	Description/Action
Management Status	Select one of the following options: • Active — When checked (the default), NA records changes to the device. • Pre-production — When checked, the device is designated as a pre-production device. A pre-production device is a device that is not yet active in the production network. Keep in mind that pre-production devices are not included in searches (unless explicitly selected to be included), and will not be included in reports on network status. (**Note**: Bare metal devices must use the Pre-production status.) • Inactive — When checked, NA does not record changes to the device. It is a good idea to select this options if the device is not supported or is not in active use. Making devices inactive reduces network traffic and frees resources.
Device Driver	Select one of the following options: • Auto Discover Driver — When checked (the default), NA queries the device using SNMP or Telnet and assigns the most appropriate device driver. (**Note**: If you are editing an existing device, the option changes to Re-discover Driver.) • Specify Driver — When checked, either the driver that is currently assigned to the device is displayed, or you can select from the list of available drivers from the drop-down menu.
Comments	Enter comments about the device.
Password Information	
Use network-wide password rules	If checked (the default), NA uses a network-wide device password rule that applies to a device. Using network-wide password rules is a highly scalable method for setting device credentials. **Note**: For large networks where groups of devices share the same credentials, use Device Password Rules. This enables you to consolidate device credentials in one place for easy manageability. Refer to “Creating Device Password Rules” on page 134 for information on creating Device Password Rules.
Use this password rule first	If checked, NA uses the password rule you select from the drop-down menu first.

Field	Description/Action
Use device-specific password information	If checked, NA uses authentication credentials that are specific to the device. Enter the following information to implement device-specific password rules. • Username — Enter the username that is used to access the device, if needed. If your devices are configured to use a AAA solution, such as TACACS+ or RADIUS, create a AAA user account and use those AAA credentials as the device credentials. • Password — Enter the password that NA uses to access the device. • Confirm Password — Enter the password again for confirmation. • Enable Password — Enter the enable password that NA needs to access privileged mode. Most configuration changes require the enable password. (**Note**: Some devices may not require a password to access the privileged mode, for example Nortel ASN/ARN. Some devices can be configured to disable the password for the privileged mode. Please check with your network administrator for site specific configurations.) • Confirm Enable Password — Enter the enable password again. • SNMP Read-Only Community String — Enter the SNMP password that NA uses to Read SNMP values. • SNMP Read/Write Community String — Enter the SNMP password that NA uses to modify Read/Write SNMP values. • SNMPv3 Username — Enter the SNMPv3 username that is used to access the device. • SNMPv3 Authentication Password — Enter the SNMPv3 authentication password that NA uses to access the device. • Confirm SNMPv3 Authentication Password — Enter the SNMPv3 authentication password again for confirmation. • SNMPv3 Encryption Password — Enter the SNMPv3 encryption password. • Confirm SNMPv3 Encryption Password — Enter the SNMPv3 encryption password again for confirmation.
Device Access Settings	
Device Access Settings	NA is designed to work with most networks and network devices. However, unique device configurations can affect NA's ability to manage certain devices. Device access settings enable you to tailor NA to adapt to your network configuration. Device access settings are tied to device password information. The device-specific settings you enter are applied only if you choose to use device-specific passwords. Network-wide device settings can be added to your password rules. Refer to "TACACS+ Authentication" on page 77 for information on TACACS+ authentication. Refer to "Logging In Using SecurID" on page 637 for information on using SecurID. **Note**: For detailed information on how to use device access settings, click the "How To Use Device Access Settings" link. The access.variables help file opens in a new browser window.
NAT Information	
NAT IP Address	Enter the internally-configured IP address of the device if it is different from the primary IP address NA uses to access the device. (**Note**: If you are using NAT, be sure to enter the IP address that NA should use to access the device in the Device IP box at the top of the page.)

Field	Description/Action
TFTP Server IP Address	Enter the NATed IP address of the NA server local to the device.
FTP Server IP Address	Enter the NATed IP address of the NA server local to the device.
Connection Information	
Connection Method	NA can communicate with your network devices using any combination of the following protocols. Select one or more protocols that you want to use. NA chooses the most efficient protocol available at any given time from those you select. • SNMP • SNMPv1 or SNMPv2c (community string authentication) • SNMPv3 (user authentication) — With SNMPv3, you have the following options: noAuthNoPriv (username only), authNoPriv (username, authentication password), and authPriv (username, authentication, and encryption password). Authentication methods include SHA (Secure Hash Algorithm) and MD5 (Message Digest Algorithm). Encryption methods include DES (Data Encryption Standard), 3DES (Triple DES), AES (Advanced Encryption Standard), AES128, AES192, and AES256. • RLogin • Telnet • SSH (You can select either SSH1 or SSH2 (the default), SSH1 Only, or SSH2 Only.) • Console Server (via Telnet) check box — In addition to the standard network connections, NA can connect to a device through a console server. Also, if the standard connections fail, the Telnet/SSH Proxy automatically fails-over to the console settings when connecting users to devices. If checked, enter the IP address or hostname of the console server, along with the port number. • Only use console server checkbox — By default, you must select at least one connection method. Telnet is used as the default. If checked, this option enables you to not check any of the above connection methods.
Transfer Protocol	Select one or more of the following transfer protocols: • SCP • SFTP • FTP • TFTP
Bastion Host	If the “Use a Unix or Linux Bastion Host for Telnet and SSH access” check box is checked, enter the: • IP address or hostname of the Bastion Host. • Username (typically root) used to access the Bastion Host. • Password used to access the Bastion Host. • Password again for confirmation. (**Note**: To modify Bastion Host information, go to “Device Managed IP Addresses Page Fields” on page 234.)

Field	Description/Action
Syslog Configuration	
Configure Syslog on Device for Configuration Change Detection	If checked (the default), and if either by driver discovery or you assigned a driver to each device, NA takes the following steps for each device: 1. Takes a snapshot of the configuration. 2. Updates the configuration to send Syslog messages to NA. 3. Writes a comment in the configuration indicating that the device was auto-configured to enable change detection. 4. Takes a final snapshot. You can select one of the following options: • Set device to log to NA Syslog Server — Checked by default if the Configure Syslog on Device for Configuration Change Detection check box is checked. • Device logs to a syslog relay, set the correct logging Level — Enter the IP address or hostname of the relay host. If a relay host has been entered before, it appears here by default.
ACL Parsing	
	Select one of the following options: • Enabled — If enabled (the default), ACL data is stored for the device upon each snapshot. Keep in mind that ACLs are not loaded in until a snapshot is taken. • Disabled — If disabled, ACL data is not stored for the device upon each snapshot.
Additional Information Keep in mind that NA populates some of the following fields automatically from the device snapshot process. If you manually populate these fields, your data is overwritten each time the device is polled.	
Device Description	Enter the description you want to use to identify the device.
Model	Enter the manufacturer’s model number for the device.
FQDN	Enter the domain to which the device belongs. This is detected if the Resolve FQDN Administration option is selected.
Serial Number	Enter the manufacturer’s serial number for the device.
Vendor	Enter the vendor of the device, for example Cisco or Nortel.
Asset Tag	Enter your company’s asset tag number for the device.
Location	Enter the physical or logical location of the device in your network.

Field	Description/Action
Hierarchy Layer	A hierarchy layer is a device attribute. You can set a device's hierarchy layer when adding or editing a device. As a result, when configuring a network diagram, you can select which hierarchy layers to filter. For example, you could select to diagram your entire network (Inventory) and then filter on “Core” to get only your Core devices—devices with a hierarchy layer set to Core. Refer to “Diagramming” on page 609 for information on diagramming your network. **Note**: The options provided below are default hierarchy layers. Refer to “Editing the appserver.rcx file” on page 617 for information on adding custom hierarchy layers.) Select a hierarchy layer from the drop-down menu. Options include: • Layer not set • Core • Distribution • Access • Edge
Custom Service Type	Enter a Service Type. Service types can specify VoIP, BGP, MPLS, and so on. The values help to identify the device’s purpose. You can use these values to tag device services so as to easily search for them or view them in a group (static or dynamic).

Edit Device Page Fields

Field	Description/Action
IP Address (or DNS name)	Displays the device’s IP address or DNS host name.
Hostname	Displays the device’s host name, if applicable.
Site <name>	Displays the Site name. Note that the field’s name can be modified on the Partitions page. (Refer to “Partitions Page Fields” on page 158 for information.) In general, a Security Partition is a grouping of devices with unique IP addresses. Multiple Security Partitions can be managed by a single NA Core. A NA Core in an installation of a NA server, comprised of a single Management Engine, associated services, and a single database. **Note**: If a Security Partition applies to a Device/Device Group, there could be additional drop-down menus for each Security Partition. (Refer to “Segmenting Devices and Users” on page 150 for information on Security Partitions.)
Belongs to Groups	Displays the group(s) to which the device will be a member. Use the Device Selector to select groups. For information on how to use the Device Selector, refer to “Device Selector” on page 144.

Field	Description/Action
Change Detection and Polling	Options include: • Enabled — When checked (the default), NA polls the device for changes as part of the regular polling task and when NA detects change events. • Polling Only — When checked, NA polls the device for changes as part of the regular polling task only. • Disabled — When checked, NA ignores change events related to the device. In addition, NA does not check the device for changes as part of the regular polling task. It a good idea to select this option during routine maintenance to exclude this device from the regular polling task.
Management Status	Options include: • Active — When checked (the default), NA records changes to the device. • Pre-production — When checked, the device is designated as a pre-production device. A pre-production device is a device that is not yet active in the production network. Keep in mind that pre-production devices are not included in searches (unless explicitly selected to be included), and will not be included in reports on network status. (**Note**: Bare metal devices must use the Pre-production status.) • Inactive — When checked, NA does not record changes to the device. It is a good idea to select this options if the device is not supported or is not in active use. Making devices inactive reduces network traffic and frees resources.
Device Driver	Options include: • Re-Discover Driver — When checked (the default), NA queries the device using SNMP or Telnet and assigns the most appropriate device driver. • Specify Driver — When checked, either the driver that is currently assigned to the device is displayed, or you can select from the list of available drivers from the drop-down menu.
Comments	Displays comments about the device.
Password Information	
Use network-wide password rules	If checked (the default), NA uses a network-wide device password rule that applies to a device. Using network-wide password rules is a highly scalable method for setting device credentials. **Note**: For large networks where groups of devices share the same credentials, use Device Password Rules. This enables you to consolidate device credentials in one place for easy manageability. Refer to “Creating Device Password Rules” on page 134 for information on creating Device Password Rules.
Use this password rule first	If checked, NA uses the password rule you select from the drop-down menu first.

Field	Description/Action
Use device-specific password information	If checked, NA uses authentication credentials that are specific to the device. Enter the following information to implement device-specific password rules. • Username — Enter the username that is used to access the device, if needed. If your devices are configured to use a AAA solution, such as TACACS+ or RADIUS, create a AAA user account and use those AAA credentials as the device credentials. • Password — Enter the password that NA uses to access the device. • Confirm Password — Enter the password again for confirmation. • Enable Password — Enter the enable password that NA needs to access privileged mode. Most configuration changes require the enable password. (**Note**: Some devices may not require a password to access the privileged mode, for example Nortel ASN/ARN. Some devices can be configured to disable the password for the privileged mode. Please check with your network administrator for site specific configurations.) • Confirm Enable Password — Enter the enable password again. • SNMP Read-Only Community String — Enter the SNMP password that NA uses to Read SNMP values. • SNMP Read/Write Community String — Enter the SNMP password that NA uses to modify Read/Write SNMP values. • SNMPv3 Username — Enter the SNMPv3 username that is used to access the device. • SNMPv3 Authentication Password — Enter the SNMPv3 authentication password that NA uses to access the device. • Confirm SNMPv3 Authentication Password — Enter the SNMPv3 authentication password again for confirmation. • SNMPv3 Encryption Password — Enter the SNMPv3 encryption password. • Confirm SNMPv3 Encryption Password — Enter the SNMPv3 encryption password again for confirmation.
Reset last used password rule	If checked, NA resets the last used password rule.
Device Access Settings	
Device Access Settings	NA is designed to work with most networks and network devices. However, unique device configurations can affect NA’s ability to manage certain devices. Device access settings enable you to tailor NA to adapt to your network configuration. Device access settings are tied to device password information. The device-specific settings you enter are applied only if you choose to use device-specific passwords. Network-wide device settings can be added to your password rules. Refer to “TACACS+ Authentication” on page 77 for information on TACACS+ authentication. Refer to “Logging In Using SecurID” on page 637 for information on using SecurID. **Note**: For detailed information on how to use device access settings, click the “How To Use Device Access Settings” link. The access.variables help file opens in a new browser window.

Field	Description/Action
NAT Information	
NAT IP Address	Displays the internally configured IP address of the device if it is different from the primary IP address NA uses to access the device. (**Note**: If you are using NAT, be sure to enter the IP address that NA should use to access the device in the Device IP box at the top of the page.)
TFTP Server IP Address	Displays the NATed IP address of the NA server local to the device.
Connection Information	
Connection Method	NA can communicate with your network devices using any combination of the following protocols. Displays one or more protocols that you are using. NA chooses the most efficient protocol available at any given time from those you select. • SNMP • SNMPv1 or SNMPv2c (community string authentication) • SNMPv3 (user authentication) — With SNMPv3, you have the following options: noAuthNoPriv (username only), authNoPriv (username, authentication password), and authPriv (username, authentication, and encryption password). Authentication methods include SHA (Secure Hash Algorithm) and MD5 (Message Digest Algorithm). Encryption methods include DES (Data Encryption Standard), 3DES (Triple DES), AES (Advanced Encryption Standard), AES128, AES192, and AES256. • RLogin • Telnet • SSH (You can select either SSH1 or SSH2 (the default), SSH1 Only, or SSH2 Only.) • Console Server (via Telnet) check box — In addition to the standard network connections, NA can connect to a device through a console server. Also, if the standard connections fail, the Telnet/SSH Proxy automatically fails-over to the console settings when connecting users to devices. If checked, enter the IP Address or Host Name of the console server, along with the port number. (To modify Console Server information when editing existing devices, go to "Device Managed IP Addresses Page Fields" on page 234.) **Note**: Connections to Cisco ASA child devices can go through the parent device. However, if the Telnet and SSH connection methods on the Cisco ASA child device do not match the parent device's connection methods, some communications could fail because the child device's connection method settings do not override the parent device's connection method settings.
Transfer Protocol	Transfer protocols include: • SCP • SFTP • FTP • TFTP
Bastion Host	To modify Bastion Host information, go to "Device Managed IP Addresses Page Fields" on page 234.)

Field	Description/Action
ACL Parsing	
	Options include: • Enabled — If enabled (the default), ACL data is stored for the device upon each snapshot. Keep in mind that ACLs are not loaded in until a snapshot is taken. • Disabled — If disabled, ACL data is not stored for the device upon each snapshot.
Additional Information Keep in mind that NA populates some of the following fields automatically from the device snapshot process. If you manually populate these fields, your data is overwritten each time the device is polled.	
Device Description	Displays a description of the device.
Model	Displays the manufacturer's model number for the device.
FQDN	Enter the Fully Qualified Domain Name (FQDN) to which the device belongs. This is detected if the Resolve FQDN Administration option is selected.
Serial Number	Displays the manufacturer's serial number for the device.
Vendor	Displays the vendor of the device, for example Cisco or Nortel.
Asset Tag	Displays your company's asset tag number for the device.
Location	Displays the physical or logical location of the device in your network.
Hierarchy Layer	A hierarchy layer is a device attribute. You can set a device's hierarchy layer when adding or editing a device. As a result, when configuring a network diagram, you can select which hierarchy layers on which to filter. For example, you could select to diagram your entire network (Inventory) and then filter on "Core" to get only your Core devices—devices with a hierarchy layer set to Core. Refer to "Diagramming" on page 609 for information on diagramming your network. **Note**: The options provided below are default hierarchy layers. Refer to "Editing the appserver.rcx file" on page 617 for information on adding custom hierarchy layers.) Select a hierarchy layer from the drop-down menu. Options include: • Layer not set • Core • Distribution • Access • Edge
Custom Service Type	A service type can specify VoIP, BGP, MPLS, and so on. The values help to identify the device's purpose. You can use these values to tag device services so as to easily search for them or view them in a group (static or dynamic).

Bare Metal Provisioning

Bare Metal Provisioning is the process of taking a device out of the box and bringing it to a state where it can function in a production network. Bare metal devices have not yet been set up to a point where they could properly interact with NA. The most common scenario for a bare metal device is one that has not yet gone through an initialization procedure, for example an interactive CLI session, that configures the device to the point where it will respond appropriately to standard NA interaction.

Note: Bare metal devices are devices that are booting up for the first time, often running some form of “bootstrap” OS. NA can only interact with the device in a very limited way when using a bare metal driver.

In general, the bare metal provisioning process includes:

- **Preparation** — During preparation, devices are brought into the system and setup to the point where they are capable of accepting configurations, firmware, OS, and so on. These devices can have a temporary location on the network, but they are not setup with the IP information that matches their intended location within the network. The goal of the preparation stage is to get the device to a known good state that can accept the type of data NA intends to provision. As a result, the device will be able to handle configuration deployment, OS deployment, and custom scripting.
- **Prototyping** — Prototyping is the process of defining and maintaining device templates. Device templates are manipulated using similar mechanisms to other devices in NA, however, there is no actual device associated with the device templates. The goal of the prototyping stage is to be able to define device configuration and other provisioning information without having to have a device to work against. The secondary goal is to provide a means to define, maintain, and reuse the information.

  Note: Device templates provide the ability to define configurations, OS/file specifications, and other device-specific information that can then be applied to existing devices. Device templates also have the ability to support certain device operations, such as policy checking without needing an actual device to test against. Refer to “Adding New Device Templates” on page 124 for information.

- **Provisioning** — During provisioning, an abstract device template is applied to a real device (usually a pre-production device). This application consists of taking the provisioning information of the device template and appropriately applying it to the device. For device template configurations, this would be a process of deploying the configuration. Provisioning also includes the ability to provide certain information that will customize the device template's provisioning information to that device. This information is similar to providing variable values for a custom script. The goal of the provisioning stage is to be able to apply the device configuration and other provisioning information of a device template to a real device.

The following outlines the bare metal provisioning steps.

1. Add the pre-production device to NA. Refer to "Adding Devices" on page 108. A pre-production device is a device that is not yet active in the production network. Keep in mind that pre-production devices are not included in searches (unless explicitly selected to be included), and will not be included in reports on network status.

   Note: You do not have to add a pre-production device to NA before configuring device templates. However, to be able to deploy a device template to a pre-production device, the device must be managed by NA.

2. Configure a device template. A device template is an abstract device configuration, including OS/file system and configuration information which can be provisioned to other devices. Refer to "Adding New Device Templates" on page 124.
3. Connect to the bare metal device. Bare metal devices are a form of pre-production devices. Functionality is very limited to making a Telnet or SSH proxy connection, running a script against the device, attempting to discover a driver, and editing device settings. Refer to "Bare Metal Provisioning Scripts" on page 577.
4. Provisioning a device from a device template. Refer to "Provision Device Task Page Fields" on page 358. Note that You can search for device templates. Refer to "Searching for Device Templates" on page 541.

Device Templates

Device templates enable you to define configurations and other device-specific information that can then be applied to existing devices. Device templates also have the ability to support certain device operations, such as policy checking, without needing an actual device to test against. Refer to "Bare Metal Provisioning" on page 118 for information on the bare metal provisioning process.

Note: Device templates are full configuration files that can be deployed to a device, completely overwriting any pre-existing data.

To access the Device Templates page, on the menu bar under Devices, select Device Tools and click Device Templates. The Device Templates page opens.

Device Template Page Fields

Field	Description/Action
New Device Template link	Opens the New Device Template page. Refer to "Adding New Device Templates" on page 124.
Check Boxes	You can use the left-side check boxes to delete device templates. Once you have selected the device template, click the Actions drop-down menu and click Delete. The adjacent Select drop-down menu enables you to select or deselect all of the device templates.
Host Name	Displays device template's host name. Clicking the host name opens the Device Template Details page, where you can view additional information for a template. Refer to "Device Template Details Page Fields" on page 121 for information.
Device Vendor	Displays the vendor of the device, for example Cisco or Nortel.
Device Model	Displays the manufacturer's model number for the device.
Partition	If you have created Partitions for security or business reasons, you can partition Device Password Rules for each device in a specific Partition. Refer to "Segmenting Devices and Users" on page 150 for detailed information on creating Partitions.
Actions	You can select the following actions: • Edit — Opens the Edit Device Template page. Refer to"Device Template Page Fields" on page 120. • View Config — Opens the View Config page. Refer to "Device Configuration Detail Page Fields" on page 177. • Test Policy Compliance — Opens the Test Policy Compliance page. Refer to "Test Policy Compliance Page Fields" on page 441 for information.

Device Template Details Page Fields

Selecting a device on the Device Template page opens the Device Template Details page for that device.

Menu Option	Description/Action
View Menu	You can select the following options: • Device Template Home — Opens the Device Template page. Refer to "Device Template Page Fields" on page 120. • Device Template Detail — Enables you to select specific Device Templates for which you want to view details. • Current Configuration — Opens the Configuration Detail page, where you can view the configuration currently set for this template and add comments. When you click the "Deploy to Device" option, you can schedule a configuration deployment or initiate an immediate configuration deployment. • Configuration History — Opens the Device Configurations page, where you can view configuration changes. Refer to "Device Configurations Page Fields" on page 175. • ACLs — Opens the Device ACLs page where you can view information on Access Control Lists (ACLs). Refer to "Viewing ACLs" on page 685 for information. • Interfaces — Opens the Device Interfaces page, where you can view information on the device's interfaces. Refer to "Device Interfaces Page Fields" on page 207 for information.
Edit Menu	You can select the following options: • Edit Configuration — Opens the Edit Configuration page with the current configuration, where you can edit the configuration and then deploy it. Refer to "Edit Template Configuration Page" on page 122 for information. • Edit Device Template — Opens the Edit Device Template page. Refer to "New Device Template Page Fields" on page 124. • Delete Device Template — Enables you to delete the Device Template. • Save As A New Template — Enables you to save the current Device Template as a new Device Template. Refer to "Device Template Page Fields" on page 120. • Process Automation — Opens the HP Operations Orchestration login page, where you can login to HP Operations Orchestration and launch HP Operations Orchestration flows in guided mode. For information on how to use HP Operations Orchestration, refer to the *HP Operations Orchestration User's Guide*.
Provision Menu	You can select the following option: • Provision Device From Template — Opens the Device Template page for the device, where you can provision a different device using the current Device Template. Refer to "Device Specific Template Page" on page 126.
Comments	Displays descriptive text for the device.
Vendor	Displays the device manufacturer's name.
Model	Displays the device's model designation.
Driver Name	Displays the driver assigned to the device.
Device Type	Displays the type of device, such as router, switch, or firewall.

Menu Option	Description/Action
Device Origin	Displays the name of the import source if the device was imported into NA and the source was named. If the import source was not named, it states Added to NA on <date>. If the device was added manually, it states Manually added by <user name> on <date>.
Last Configuration Change	Displays the date and time the device's configuration was last changed.
Management Status	Since device templates are not actual devices, and therefore cannot be designated as Active or Inactive, Device Template is displayed.

Edit Template Configuration Page

A Device Template's configuration is essentially a script that can be used to replace a device's entire configuration file. The configuration should therefore be a complete working configuration file that a device can use at boot time.

Instead of creating a configuration from scratch, you can copy the configuration from a device already on your network using the "Save As New Template" command. Refer to "Edit Menu Options" on page 232 for information.

Variables can be used to customize the configuration. Note that the `'$'` character is reserved for the variable name. Use escape sequence `\x24` if you need to enter a literal `'$'` in a Device Template.

Note: Variables beginning with the `tc_` are reserved for special use. You cannot define any variables that begin with that character sequence.

Custom variables, such as `$MyVar$` can have prompts defined for them using the Pull Variables button. The Pull Variables button refreshes the page, adding input fields at the bottom of the page for each variable used in the Device Template. Use these fields to define custom prompts for the variables and to limit the values that each prompt will accept:

- Allow multiple lines in value
- Limit Values To: (first, last, next-to-last)
- Password (If checked, NA does not echo the password when prompting for a value on the Run Command Script Task page.

Reserved variables, such as `$tc_device_hostname$` are automatically filled in with the value from the device or devices being provisioned. The values from the Device Template itself are not used for these variables.

Note: If you would rather have custom variables supplied in a CSV file, you can replace the existing scriptField1, scriptFiled2, and so on headers with the names of the custom variables from your Device Template. Using a CSV file enables a Device Template to provision several devices at once. Be sure to provide variable values for each device to be provisioned with the Device Template.

Changing a Device's Primary IP Address

If you want to change a device's Primary IP Address as part of the Device Template Provisioning process, there is a special reserved variable for this purpose and used only for Device Templates: `$tc_device_primary_ip$`. Unlike other reserved variables, its value is supplied by you when the Provision Device task runs or in a CSV file. The CSV data file includes this variable as a column.

If you include `$tc_device_primary_ip$` in your Device Template's configuration, after the Provision Device task completes, NA updates the Primary IP Address used to access the device to this new value. NA will display the new Primary IP Address to identify the device in all reports and searches.

Adding New Device Templates

The New Device Template page enables you to add a new device template.

To add a new device template, on the menu bar under Devices, select New and click Device Template. You can also access this page from the New Device Template link on the Device Templates page. The New Device Template page opens.

New Device Template Page Fields

The New Device Template page enables you to configure a device template.

Note: The Edit Device Template page is identical to the New Device Template page, except that the fields are populated.

Field	Description/Action
Name	Enter the device template's name.
Partition	Select a Partition from the drop-down menu, if applicable. Keep in mind that the new device template will only apply to the devices in the Partition. Refer to "Segmenting Devices and Users" on page 150 for detailed information on creating Partitions.
Device Driver	Select a driver from the list of available drivers from the drop-down menu
Comments	Enter comments about the device.
Connection Information (Note that although a device template is not an actual device, and cannot be connected to itself, devices that are provisioned from the device template can inherit these connection settings. Refer to "Device Templates" on page 120 for information.)	
Connection Method	NA can communicate with your network devices using any combination of the following protocols. Select one or more protocols that you want to use. NA chooses the most efficient protocol available at any given time from those you select • SNMP • SNMPv1 or SNMPv2c (community string authentication) • SNMPv3 (user authentication) — With SNMPv3, you have the following options: noAuthNoPriv (username only), authNoPriv (username, authentication password), and authPriv (username, authentication. and encryption password). Authentication methods include SHA (Secure Hash Algorithm) and MD5 (Message Digest Algorithm). Encryption methods include DES (Data Encryption Standard), AES (Advanced Encryption Standard), AES192, and AES256. • RLogin • Telnet • SSH (You can select either SSH1 or SSH2 (the default), SSH1 Only, or SSH2 only.)
Transfer Protocol	Select one or more of the following transfer protocols: • SCP • FTP • TFTP

Field	Description/Action
ACL Parsing	
	Select one of the following options: • Enabled — If enabled (the default), ACL data is stored for the device upon each snapshot. Keep in mind that ACLs are not loaded in until a snapshot is taken. • Disabled — If disabled, ACL data is not stored for the device upon each snapshot.
Additional Information Keep in mind that NA populates some of the following fields automatically from the device snapshot process. If you manually populate these fields, your data is overwritten each time the device is polled.	
Device Description	Enter the description you want to use to identify the device.
Model	Enter the manufacturer’s model number for the device. The Resolve FQDN task enables you to set the FQDN (Fully Qualified Domain Name) for each device in the system by running a reverse DNS lookup on the device’s primary IP address.
Vendor	Enter the vendor of the device, for example Cisco or Nortel.
Hierarchy Layer	A hierarchy layer is a device attribute. You can set a device's hierarchy layer when adding or editing a device. As a result, when configuring a network diagram, you can select which hierarchy layers on which to filter. For example, you could select to diagram your entire network (Inventory) and then filter on “Core” to get only your Core devices—devices with a hierarchy layer set to Core. Refer to “Diagramming” on page 609 for information on diagramming your network. **Note**: The options provided below are default hierarchy layers. Refer to “Editing the appserver.rcx file” on page 617 for information on adding custom hierarchy layers.) Select a hierarchy layer from the drop-down menu. Options include: • Layer not yet set • Core • Distribution • Access • Edge
Custom Service Type	Enter a Service Type. Service types can specify VoIP, BGP, MPLS, and so on. The values help to identify the device’s purpose. You can use these values to tag device services so as to easily search for them or view them in a group (static or dynamic).

Be sure to click the Save button when you are finished or the Save And Add Another button if you want to add another device template.

Device Specific Template Page

When you select the Provision Device From Template option from the Provision menu on the Device Template Details page, the Device Template page opens for that device. This page shows a list of devices that match the driver assigned to the device template, which can be provisioned from the device template.

Field	Description/Action
Display Devices	Select one of the following options from the pull-down menu: • All • Active • Pre-production
Host Name	Displays the host name of the device. Clicking a host name opens the Device Detail page, where you can view information about the device and its configuration history.
Device IP	Displays the IP address of the device. Devices in red failed the last snapshot attempt. Inactive devices are marked with an icon beside the IP address. Clicking an IP address opens the Device Detail page, where you can view information about the device and its configuration history.
Device Vendor	Displays the name of the device manufacturer.
Device Model	Displays the model designation of the device.
Partition	Select a Partition from the drop-down menu, if applicable. Keep in mind that the new device template will only apply to the devices in the Partition. Refer to "Segmenting Devices and Users" on page 150 for detailed information on creating Partitions.
Actions	You can select the following options: • Provision Device — Opens the New Task - Provision Device page, where you can provision the device. Refer to "Provision Device Task Page Fields" on page 358. • Compare Configuration — Opens the Compare Device Configurations page. Refer to "Compare Device Configurations Page Fields" on page 181.

Using the New Device Wizard

To add devices using the New Device Wizard, on the menu bar under Devices, click New Device Wizard. The New Device Wizard opens.

New Device Wizard Page Fields

Step	Description/Action
Step 1: Create Device	Enter the following information: • Hostname or IP — Enter the host name or IP address of the device. • Comments — Enter any comments about the device. • Management Status — Select either Active or Inactive. (**Note**: Pre-production devices cannot be added via the New Device Wizard.) When you are finished, click either: • Next — Opens the Authenticate page. (See below) • Finish — If the device was successfully added, the Add Device Wizard Congratulations page opens. This page provides information on any discovery issues.
Step 2: Authenticate Device	Select one of the following options: • Use network-wide password rules — If checked (the default), NA uses a network-wide device password rule that applies to the device. You can click the Create One link to create a network-wide password rule. Refer to "Creating Device Password Rules" on page 134. • Use device-specific password — If checked, enter the following information for the device: Username, Password, Enable Password (if applicable), SNMP Read Community String, and SNMP Write Community String. For SNMPv3, enter authentication and encryption information. When you are finished, click either: • Back — You are returned to the Create Device step. • Next — Opens the Configure page. (See below) • Finish — If the device was successfully added, the Add Device Wizard Congratulations page opens. This page provides information on discovery issues.
Step 3: Configure Device	NA attempts to discover the vendor and model of the device. If successful, NA retrieves and stores the device configuration. The device is then configured for change detection. If you do not want to configure the device for change detection, uncheck the Update Syslog Configuration on Device box. If the box is checked, select one of the following options: • Log to HP Network Automation's Syslog Server — Checked by default if the Update Syslog Configuration on Device box is checked. • Log to existing Syslog Relay Host — Enter the host name or IP address of the relay host. (**Note**: NA will set the correct logging level for change detection.) Click Finish. If the device was successfully added, the Add Device Wizard Congratulations page opens. This page provides information on any discovery issues.

Importing Devices

There are several ways to import devices from a comma-separated values (CSV) file:

- Using device password rules (usually assigned to group) and a CSV file.
- Importing device data in one CSV file and device password information in another CSV file.

To import devices using CSV files, on the menu bar under Devices, select Device Tasks and click Import. The Import Task page opens. Refer to "Import Devices Task Page Fields" on page 331.

NA can be configured to regularly import devices from a CSV file. The first time you import devices, you will have to:

- Set up the Device Password Rules and have them applied to the Inventory group (all devices). Refer to "Creating Device Password Rules" on page 134.
- Configure the default connection method. Refer to "Device Access Page Fields" on page 47.
- Prepare the device import file (Device.csv). Keep in mind you can edit the Device.csv file or load it into a program such as Excel. Refer to "Creating CSV Files for Importing Device Data" on page 128.

Note: The Detect Network Devices task enables you to locate devices on your network that you want to place under NA management. Once you provide a range of IP addresses, NA scans your network looking for devices. Refer to "Detect Network Devices Task Page Fields" on page 343 for information.

To import devices using groups and device password rules, make sure you have:

1. Defined groups for the devices you are importing. Refer to "Adding Device Groups" on page 138.
2. Defined network-wide password rules for each group. Refer to "Creating Device Password Rules" on page 134.
3. Created a *device.csv* file that includes the group to which each device belongs. See "Creating CSV Files for Importing Device Data" on page 128.
4. Discovered drivers for the imported devices. Refer to "Discovering Device Drivers" on page 165. Refer to the Driver Release Service (DRS) documentation for detailed information on supported devices. The DRS is an automated driver release and delivery system.

Creating CSV Files for Importing Device Data

Use the import device data task to import information about devices, device groups, or device passwords into NA from CSV files. The first row of the CSV file contains the NA database column names for the data you are importing. Each additional row represents one device, device group, or device-specific password.

NA provides templates for the CSV files. Note the following:

- Do not include columns unless you are populating them. An empty value overwrites existing data if the device already exists.
- The column names must match the database column names. Do not change the database column names set by NA.
- Because the data fields are comma-delimited, fields can include whitespace but not commas (,). Use a colon (:) to separate values within a field.
- Column order is not significant.

To create a CSV file for import:

1. Navigate to the New Task/Template - Import Devices page.
2. Under Task Options, Data Type, click the appropriate CSV template link.
3. In an editing tool, do the following:
   - Add information to the data table.
   - To prevent overwriting existing data, delete any unused columns.
   - For information about the columns in the CSV file, see the appropriate section:
     - "Device Data Import File" on page 129
     - "Device Group Data Import File" on page 132
     - "Device-Specific Password Data Import File" on page 133

   Note: For a CSV file containing non-English characters, edit the file in a text editor, not Microsoft Office Excel. Save the CSV file with UTF-8 encoding.

4. Save the file as type CSV on the local system.

Device Data Import File

The *device.csv* template file contains the NA database column names for device data. During import, NA uses the values in the primaryIPAddress and hostName columns, combined with the values in the optional siteName column, to uniquely identify devices in the database. Populate at least one of the primaryIPAddress or hostName columns.

Device Import File Fields

Column Name	Description/Action
primaryIPAddress	The primary IP address for the device. Either the primaryIPAddress or the hostName column must be included in each device data import file. (**Note**: In a NAT environment, specify the IP address that NA should use to access the device.) **Note**: This value can be set at device creation only.

Device Import File Fields (cont'd)

Column Name	Description/Action
hostName	The host name of the device. Either the primaryIPAddress or the hostName column must be included in each device data import file. **Note**: This value can be set at device creation only.
siteName	The name of the site (partition) to which the device belongs. **Note**: This value can be set at device creation only. It takes precedence over the Site selected on the Import Devices task page.
deviceGroupName	A colon-separated list of the device groups that contain the device. If a device group name does not exist, NA creates that device group with default properties.
deviceDriver	The name of the device driver. **Tip**: It is recommended to not specify a device driver and let NA determine which driver to use.
excludeFromPoll	The polling setting for the device. Specify one of the following numeric values: • 1 — Disabled (do not poll the device automatically) • 2 — Polling Only (poll the device for changes as part of the regular polling task only)
managementStatus	The management status of the device. Specify one of the following numeric values: • 0 — Active (managed) • 1 — Inactive (not managed) • 3 — Pre-production (not yet fully configured)
nATIPAddress	The internally-configured IP address of the device, if different from the primary IP address NA uses to access the device.
tFTPServerIPAddress	The IP address of the TFTP server local to the device.
accessMethods	The connection methods for the device. This value is constructed as follows: access_methods[+connect_methods[+console]], for example: • CLI:TFTP+ssh+console • CLI:FTP+ssh:telnet • SNMP:TFTP The value of accessMethods can be CLI, SNMP, TFTP, or FTP, and colon-delimited if more than one access method is supported. (**Note**: connect_methods only applies if CLI is supported, and can be SSH or Telnet, and colon-delimited if more than one method is supported.) For more information, see "Connection Method" on page 124.
consoleIPAddress	The IP address of the console associated with the device.
consolePort	The port number for the console. (**Note**: Only Telnet is used to access console server.)

Device Import File Fields (cont'd)

Column Name	Description/Action
deviceName	The description that identifies the device. **Note**: NA updates this value with each device poll.
model	The manufacturer's model number for the device. **Note**: NA updates this value with each device poll.
primaryFQDN	The domain to which the device belongs.
serialNumber	The manufacturer's serial number for the device.
vendor	The vendor of the device, for example Cisco or Nortel. **Note**: NA updates this value with each device poll.
assetTag	Your company's asset tag number for the device.
geographicalLocation	The physical or logical location of the device in your network.
performACLParsing	The ACL parsing setting for the device. Specify one of the following numeric values: • 0 — Enabled (parse and store ACL data with each snapshot) • 1 — Disabled (do not parse ACL data with each snapshot)
hierarchyLayer	The hierarchy layer for the device. Specify one of the following numeric values: • 1 — Core • 2 — Distribution • 3 — Access • 4 — Edge **Note**: If additional hierarchy layers are configured, other values are possible. For more information, see "Editing the appserver.rcx file" on page 617. **Note**: NA updates this value with each device poll.
comments	Additional information about the device. Do not include commas (,).
deviceCustom[1-6]	If additional device fields are defined on the Custom Data Setup page, you can import data for any of those fields. Use the column headings as defined in the template file.
<enhanced custom field name>	If enhanced custom fields are enabled and defined for devices, you can import data for any of those fields. Add one column for each field for which to import data. Set the column headings to the actual name of the enhanced custom fields in the NA database.

Device Group Data Import File

The *device_group.csv* template file contains the NA database column names for device group data. During import, NA uses the values in the deviceGroupName column to uniquely identify device groups in the database.

Device Group Import File Fields

Column Name	Description/Action
deviceGroupName	The name (255 character maximum) of the device group. This column must be included in each device group data import file. **Note**: This value can be set at device group creation only.
siteName	The name of the site (partition) to which the device group belongs.
comments	Description text (255 character maximum) about the device group. Do not include commas (,).
isParent	The parent specification of the device group. Specify one of the following numeric values: • 0 — Not a parent (does not contain other device groups) • 1 — Parent (contains other device groups)
shared	The visibility setting of the device group. Specify one of the following numeric values: • 0 — Private (visible only to the group owner and the System Administrator) • 1 — Public (visible to all users)
parentDeviceGroupName	The name of the parent device group to which the device group belongs. **Note**: This value must be a public device group.
deviceGroupCustom[1-6]	If additional device groip fields are defined on the Custom Data Setup page, you can import data for any of those fields. Use the column headings as defined in the template file.

Device-Specific Password Data Import File

The *device_auth.csv* template file contains the NA database column names for device-specific password data. During import, NA uses the values in the deviceIPAddress column to uniquely identify devices in the database.

Device-Specific Password Data Import File Fields

Column Name	Description/Action
deviceIPAddress	The primary IP address for the device. This column must be included in each device password data import file.
readCommunityString	The SNMP read-only community string.
writeCommunityString	The SNMP read/write community string.
localUserName	The username that NA uses to access the device. If your devices are configured to use a AAA solution, such as TACACS+, create a AAA user account for NA and use those AAA credentials as the device credentials.
localPassword	The password that NA uses to access the device.
enablePassword	The enable password that NA needs to access privileged mode.

Creating Device Password Rules

Device password rules enable you to apply the same username, password, and SNMP community strings to groups of devices, IP address ranges, or host names.

Note: Device password rules can only be applied to “public” device groups. You cannot apply a password rule to “private” device groups

When attempting to login to a device, NA applies the applicable Device Password Rules list sequentially until the login succeeds, and then sets that rule as the device login. If the rule fails during a future login attempt, NA tries the applicable rules again in sequence until it finds a new valid login. This is configurable on the Device Access page. Refer to “Device Access Page Fields” on page 47 for information.

Note: The “Always try last successful password first” and “Always try passwords in defined order” options can be set when creating device passwords. Refer to “Device Access Page Fields” on page 47 for information.

To create Device Password Rules, on the menu bar under Devices select Device Tools and click Device Password Rules. The Device Password Rules page opens.

Note: The order of rules is significant. NA applies rules in the order shown on the Device Password Rules page. If you notice a persistent performance problem when taking snapshots, consider reordering the rules to place the most commonly-used rules at the top. You should also restrict rules to fewer groups or smaller IP ranges.

Device Password Rules Page Fields

Field	Description/Action
New Password Rule link	Opens the Device Password Rule page. You can use this page to create and edit device password rules. Refer to “Device Password Rule Page Fields” on page 136 for information.
Check Boxes	You can use the left-side check boxes to delete device password rules. Once you have selected the rules, click the Actions drop-down menu and click Delete. The adjacent Select drop-down menu enables you to select or deselect all of the rules.
Change Date	Displays the date and time the rule was last changed.
Rule Name	Displays the name of the rule.
Type	Displays the type of rule, either: • IP Range • Host Name • Device Group

Field	Description/Action
Partition	If you have created Partitions for security or business reasons, you can partition Device Password Rules for each device in a specific Partition. Keep in mind that you can configure Device Password Rules to be shared by all devices in all Partitions, as well as for specific devices in specific Partitions. If the Device Password Rule is available to all Partitions, it is labeled [Shared]. Refer to "Segmenting Devices and Users" on page 150 for detailed information on creating Partitions. **Note**: When creating Device Password Rules, you can select a Partition from the drop-down menu. Refer to "Device Password Rule Page Fields" on page 136 for information.
Devices	Displays the rule's host name, IP address, or group name.
Created By	Displays the login name of the person who modified the rule. NA means the name is not available.
Actions	You can select the following action for each rule: • Edit — Opens the Device Password Rule page, where you can edit the rule. Refer to "Device Password Rule Page Fields" on page 136 for information. (**Note:** Device Password Rules are listed in priority order. Use the arrows to move the rule up or down in the list.)

Device Password Rule Page Fields

Note: Passwords and SNMP community strings are stored in the NA database encrypted.

Field	Description/Action
Rule Definition	
Network-Wide Password Rule	If checked (the default), NA uses a network-wide device password rule that applies to all devices in the rule. Using a network-wide password rule is a highly scalable method for setting device credentials.
Rule Name	Enter the rule name.
Partition	Select a Partition from the drop-down menu, if applicable. Keep in mind that the Device Password Rule will only apply to the devices in the Partition. Refer to "Segmenting Devices and Users" on page 150 for detailed information on creating Partitions.
Insert Before	Select an existing rule name from the drop-down menu that this rule is to be inserted above.
IP Range	If checked, enter the first and last IP addresses of the range to which the rule applies. Using wildcards (* or ?), you can apply this rule to a set of related devices.
Hostname	If checked, enter the host name for which this rule applies. Using wildcards (* or ?), you can apply this rule to a set of related devices.
Device Group	If checked, select the name of one group using the Device Selector to which this rule applies. To apply the rule to all devices, select Inventory. Remember that device password rules can only be assigned to a single device group.
Device-Specific Password Information	If checked, enter a device IP address. NA takes the current authentication information on this page and copies it to the specified device when you click the Save button.
Password Information	
Username	Enter the username that NA uses to access the device. If your devices are configured to use a AAA solution, such as TACACS+, create a AAA user account for NA and use those AAA credentials as the device credentials.
Password	Enter the password that NA uses to access the device.
Confirm Password	Enter the password again for confirmation.
Enable Password	Enter the enable password that NA needs to access privileged mode. Most configuration changes require the enable password. (**Note**: Some devices may not require a password to access the privileged mode, for example Nortel ASN/ARN. Some devices can be configured to disable the password for the privileged mode. Please check with your network administrator for site specific configurations.)
Confirm Enable Password	Enter the enable password again for confirmation.
SNMP Read-Only Community String	Enter the SNMP read-only community string.

Field	Description/Action
SNMP Read/Write Community String	Enter the SNMP read/write community string.
SNMPv3 Username	Enter the SNMPv3 username that is used to access the device.
SNMPv3 Authentication Password	Enter the SNMPv3 authentication password that NA uses to access the device.
Confirm SNMPv3 Authentication Password	Enter the SNMPv3 authentication password again for confirmation.
SNMPv3 Encryption Password	Enter the SNMPv3 encryption password.
Confirm SNMPv3 Encryption Password	Enter the SNMPv3 encryption password again for confirmation.
Show Device Access Settings	NA is designed to work with most networks and network devices. However, unique device configurations can affect NA's ability to manage certain devices. Device access settings enable you to tailor NA to adapt to your network configuration. Device access settings are tied to device password information. The device-specific settings you enter are only applied if you choose to use device-specific password information. Network-wide device settings can be added to your password rules. Examples include: • Exec mode prompt • Config mode prompt • Admin prompt **Note**: When defining device password rules, although you are able to define multiple values for each device access setting, you should only specify one value per device access setting. If you specify a device access setting more than once, only one of the values is used, and there is no specific determination of which value will be used. For detailed information on how to use device access settings, click the "How To Use Device Access Settings" link.

Be sure to click the Save button when you are finished. The new rule is displayed in the Device Password Rules list.

Adding Device Groups

Creating a device group helps you categorize your devices in ways that make sense for your organization. Your devices are probably organized already, perhaps using one of the following schemes:

- Geography/physical location, such as Seattle and New York
- Business unit/department, such as Sales, Purchasing, and Manufacturing
- Role in the network architecture, such as core, edge, distribution, and access

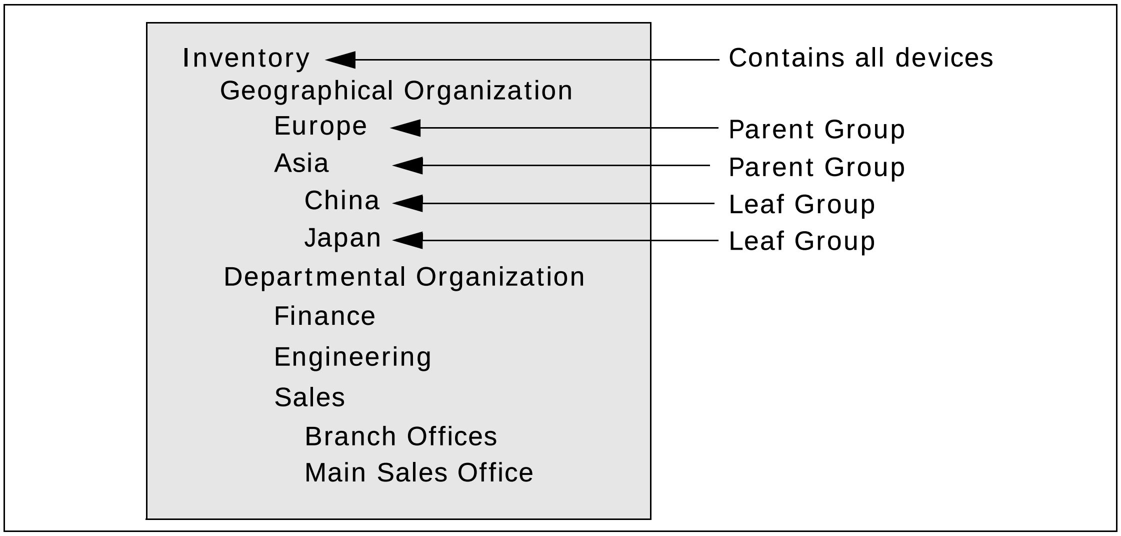
Initially, the Device Groups page includes one system group, the Inventory group. The Inventory group contains all devices added to NA. However, any user-defined groups you create also appear on this page.

A device group hierarchy in NA is made up of parent groups and leaf groups.

- A parent group can only have one parent. Any previous association is overwritten if you add a parent group as a child group of a new parent group. In addition, a parent group can contain only device groups, not devices.
- A leaf group can contain only devices, not other device groups.

Keep in mind that the default Inventory group is treated specially and is both a parent and a leaf group. It contains all devices in the system. Any leaf groups that do not belong to a parent group are included in the Inventory group.

Creating a device group hierarchy enables you to easily run tasks and reports against a set of device groups. An example device group hierarchy is shown below.


Inventory
Geographical Organization
Europe
Asia
China
Japan
Departmental Organization
Finance
Engineering
Sales
Branch Offices
Main Sales Office
Contains all devices
Parent Group
Parent Group
Leaf Group
Leaf Group

With this device group hierarchy, for example, you can run tasks and reports against the Japan devices or against the Asia devices (which would include all of the China and Japan devices).

New Group Page Fields

To add new device groups, on the menu bar under Devices select New and click Device Group. The New Group page opens.

Note: Unless you are the NA administrator, you cannot grant “Manage View” or “Manage Partition” permissions to a user group.

Field	Description/Action
Group Name	Enter a group name
Description	Enter a description of the group.
Site <name>	Select a Partition from the drop-down menu, if applicable. Note that the field name can be modified on the Partitions page. (Refer to “Partitions Page Fields” on page 158 for information.)
Owner	Select a name from the drop-down menu. Admin is the default.
Sharing	Select either Public or Private. All users can see Public groups, while only the group owner and the System Administrator can see Private groups. **Note**: With private device groups, multiple users can set up their own device groups. When they log into NA, they only see their device groups, as well all public device groups. As a result, users can customize NA for ease-of-use and scalability.
Parent Device Group	The Inventory group appears in the drop-down menu, but you can select another group. Keep in mind that your selection is ignored if you make the group private. Private groups cannot be part of the group hierarchy.
Devices	Select one of the following options: • Use Device Selector to select a fixed device set (static group) — For information on how to use the Device Selector, refer to “Device Selector” on page 144. • Use filters to define a dynamic device set (dynamic group) — Refer to “Dynamic Device Groups” on page 142 for information.

Adding Parent Groups

To add a new parent group:

1. On the menu bar under Devices click Groups. The Device Group page opens. Refer to "Device Groups Page Fields" on page 147.
2. Click the New Parent Group link at the top of the page. The New Parent Group page opens.

Note: You must have the correct permissions to create parent groups. Also, the device group hierarchy is shared and all parent groups must be made public.

New Parent Group Page Fields

Field	Description/Action
Group Name	Enter the name of the parent group.
Description	Enter a description of the parent group, which usually differentiates this from other groups.
Site <name>	Select a Partition from the drop-down menu. Note that the field name can be modified on the Partitions page. (Refer to "Partitions Page Fields" on page 158 for information.)
Sharing	Parent groups are always public.
Parent Device Group	Inventory is displayed by default in the drop-down menu.
Child Device Groups	• All device groups — Displays a list of all current device groups. Select the device groups you want to include as children of the parent group and click Copy >>. Keep in mind that a group can only be a child of one parent group. If the group you are adding already belongs to a parent group, the group will be removed from the former parent group. • Children of this group — Displays a list of device groups that are assigned to the parent group as children. Select the child groups you want to remove from this parent group and click << Remove.

When you are finished, click the Save button. The Parent Group opens.

Parent Group Page Fields

Field	Description/Action
New Group link	Opens the New Group page, where you can create a new device group. Refer to "Adding Device Groups" on page 138 for information.
New Parent Group link	Opens the New Parent Group page, where you can add a new parent group. Refer to "New Parent Group Page Fields" on page 140 for information.
Group Name	Displays the user-defined name of the device group. Clicking a group name opens the Device Group Details page. Refer to "Device Group Details Page Fields" on page 148 for information.
Description	Displays a description of the group, which usually differentiates this from other groups.
Number of devices	Displays the number of devices in the group.
Owner	Displays the user name that created the device group.
Sharing	Displays whether the group is Public or Private. All users can see Public groups, while only the group owner and the System Administrator can see Private groups.
Actions	You can select the following options: • View — Displays the devices contained in the selected device group. The devices can either be direct children of this device group if this is a leaf device group, or they could be children of child groups if the device group is a parent device group. Refer to "Viewing Device Groups" on page 146 for more information on the View option. • Edit Group — Opens the Edit Group page, where you can change the name and comments for a user-defined group. You can also add and delete devices from the group. Refer to "Edit Group Page Fields" on page 162 for information. • Delete — Permanently deletes a group. • Diagram — Opens the Diagramming page. Refer to "Diagramming" on page 609. • Make Public/Private — Toggles a device group between Public and Private modes.

Dynamic Device Groups

A dynamic device group is very similar to a static device group, except the devices included in a dynamic device group are not fixed. Rather, the system determines which devices are included in a dynamic device group by doing a query using predefined criteria associated with the group.

As with static device groups, dynamic device groups are displayed in all group lists, including Run Device tasks pages, Search pages, Diagrams, Device Software reports, and so on. The following table outlines the differences between static and dynamic device groups.

Static Device Groups	Dynamic Device Groups
Created by selecting devices. Refer to "New Group Page Fields" on page 139.	Created by defining a set of search criteria and/or rules. The maximum search criteria is 10. The steps for creating a dynamic device group are listed below.
Devices remain fixed unless manually added or removed.	Devices can change when network and/or device configuration events occur.
Can manually remove devices from the group.	Cannot manually remove devices from the group.

Note: A dynamic group can only be a child group in the group hierarchy. In addition, dynamic groups do not appear on the Edit Device page or the Import Device Task page, where you specify to which group devices belong.

Creating Dynamic Device Groups

There are two ways to create a dynamic device group:

- Using the Device Search Results page
- Using the New Group page

To create a dynamic group using the Device Search page:

1. On the menu bar under Reports, select Search For and click Devices. The Search For Device page opens.
2. Enter search criteria. For example, check the Device Vendor field and enter Cisco.
3. Click the Search button. The Device Search Results page opens displaying all of your Cisco devices.
4. Scroll down to the bottom of the page until you see the yellow "Search Criteria" section.
5. Enter the name of the dynamic group, check the "Create as a dynamic group" option, and click the Create Group button.
6. The "Successfully created new device group: <name>" message is displayed at the top of the Device Search Results page.

To create a dynamic group using the New Group Page:

1. On the menu bar under Devices, select New and click Device Group. The New Group page opens.
2. Enter the name of the dynamic group in the Group Name field.
3. Complete the Description, Partition name (if applicable), Owner, Sharing, Parent Device Group, and Devices fields as needed. Refer to "New Group Page Fields" on page 139 for details on these fields.
4. Scroll down to the Devices field.
5. Click the "Use filters to define a dynamic device set (dynamic group)" option. The display changes enabling you to:
   - Configure searches using one or more search criteria, for example Device IP, Domain Name, Policy Compliance, and so on. (**Note**: You must specify at least one search filter and/or rule to create a dynamic device group.)
   - Create a Boolean expression using the AND and OR operators to filter searches, if necessary.

     Note: This tool does not support the use of regular expresssions.
   - Limit a search by device group. Using this option, you can create a dynamic group based on other groups.
6. Once you have defined your dynamic device group, click the Save button. The new dynamic device group is displayed.

To change a dynamic device group to a static device group, open the Edit Group page and scroll down to the Device field. Click the "Use Device Selector to select a fixed device set (static group)" option. When you change a dynamic device group to a static device group, the current devices become the members of the new static device group.

Calculating Dynamic Device Groups

A dynamic device group's members are calculated when:

- You first configure the dynamic device group.
- You click the "Update device list" link on the Dynamic Device Group page.
- A background process periodically re-calculates all of the dynamic device groups.
- Pre-defined device change events occur.

Refer to "Server" on page 54 for information on the Dynamic Group Auto-Recalculation and Event Driven Recalculation parameters.

Device Selector

The Device Selector includes two options:

- Device selection — Enables you to easily navigate group trees to select devices for a variety of applications, for example when scheduling tasks on devices.
- Device group selection — Enables you to easily navigate group trees to select device groups for a variety of applications, for example when editing device groups.

Each of these selectors opens a window, enabling you to navigate devices and device groups.

Selecting Devices

By default, the Device Selector is closed. To quickly browse a fixed device or device group, you can enter the first few characters of an IP address, hostname, or device group name. Search results are displayed immediately after the first character is entered.

To select from the auto-complete list:

- For a single item — Click the item, or press the down arrow to highlight an item, and then press the Enter key.
- For multiple items — Press the Ctrl key, select the desired items, and press the Enter key.

To de-select from the auto-complete list:

- For a single item — Click the red X icon displayed to the right of the item.
- For multiple items — Press the Ctrl key, select the desired items, and Click the red X icon displayed to the right of the items.

If you are searching by prefixing a Partition name, for example, `Default Site:10.255.1.10`, the auto-complete list displays just the Partition name until the full name has been entered. For example, if you enter `Def`, you will not see the complete Partition name, `Default Site:10.255.1.10`, until the full Partition name is entered.

Selecting Device Groups

To browse for device groups, click the magnifying glass icon. The Device Group Selector window opens and displays the device groups hierarchy with the Inventory device group listed first.

The device group hierarchy is collapsed by default. You can expand it by clicking the plus (+) sign. A single click on a device group displays all of the devices in that group. If there are more entries than can be displayed, a vertical scroll bar is displayed.

To view a list of all devices in a device group, click the name of the device group. The following information is displayed.

Field	Description/Action
Filter	Enables you to quickly browse a device group.
Host Name	Displays the host name of the device.
Device IP	Displays the IP address of the device.
Device Vendor	Displays the name of the device manufacturer.
Device Model	Displays the model designation of the device.
Partition	Displays the Partition to which the device group belongs. Partitions are a set of NA objects. Partitions can be used in conjunction with a permissions model, group hierarchy, distribution of devices across NA Cores, and network diagramming. Refer to “Partitions” on page 158 for more information.

Device Selector Buttons

Use the following Device Selector buttons:

- Apply button — To select one or more devices or device groups, click the desired entries in the display (they become highlighted), and click the Apply button. The selected items are added and the Device Selector or Device Group Selector window remains open. If any of the selected devices or device groups are not allowed, the Apply button is grayed out.
- OK button — Adds the currently selected items and closes the Device Selector or Device Group Selector window. If any of the selected devices or device groups are not allowed, the OK button is grayed out.
- Cancel button — Closes the Device Selector or Device Group Selector window without saving any changes.

Note: There are resize icons at the top-right corner of Device Selector and Device Group Selector windows. You have the option of maximizing and restoring to original size, respectively.

Viewing Device Groups

Initially, the Device Groups page includes one system group: the Inventory group. The Inventory group contains all devices. However, any user-defined groups you create also appear on this page.

The View action link displays the devices contained in the selected device group. The devices can either be direct children of a device group if the device group is a leaf device group, or they could be children of child groups if the device group is a parent device group.

In previous NA releases, you could only view a leaf group's devices by clicking the device group's name. Now, you can click the View action link to see a listing of devices from the perspective of any of the parent groups in its ancestry. This enables batch editing of devices from the desired parent group's perspective.

For example, if you had device groups organized by state, then by county, and then by city, you can now do batch edits on all the devices at the state level, whereas previously you could only do batch edits on devices at the city level. Refer to “Adding Device Groups” on page 138 for detailed information on adding device groups.

To view device groups, on the menu bar under Devices, click Groups. The Device Groups page opens. Keep in mind that Public device groups are visible to all users. Private device groups are visible only to the group owner and NA administrators.

Device Groups Page Fields

Field	Description/Action
New Group link	Opens the New Group page, where you can create a new device group. Refer to "Adding Device Groups" on page 138 for information.
New Parent Group link	Opens the New Parent Group page, where you can add a new parent group. Refer to "New Parent Group Page Fields" on page 140 for information.
Group Name	Displays the user-defined name of the device group. Parent groups are not indented, unless they are also children of other parent groups. Groups that belong to a parent group are indented beneath their parent. Clicking a group name opens the Device Group page, where you can view detailed information about the device group. Refer to "Device Group Details Page Fields" on page 148 for information.
Description	Displays a description of the group.
Number of devices	Displays the number of devices in the group.
Owner	Displays the user name that created the device group.
Sharing	Displays whether the group is Public or Private. All users can see Public device groups, while only the group owner and the NA Administrator can see Private device groups.
Actions	The Actions field for the Inventory group is empty until you select a group name. User-defined groups display the following actions: • View — Displays the devices contained in the selected device group. The devices can either be direct children of this device group if this is a leaf device group, or they could be children of child groups if the device group is a parent device group. • Edit — Opens the Edit Group page, where you can change the name and comments for a user-defined group. You can also add and delete devices from the group. Refer to "Edit Group Page Fields" on page 162 for information. • Delete — Permanently deletes the group. • Diagram — Opens the Diagramming page. Refer to "Diagramming" on page 609. • Make Public/Private — Toggles a device group between Public and Private modes.

Note that the device group's tree includes a tooltip that shows the device groups partition membership. This information can be used to help differentiate between duplicate device group names and for setting up device group partitions.

For example, if you are creating multiple partitions and multiple user groups that have View permissions set to those partitions, two device groups could have the same name when you view the Device Groups page. Using the tooltip, you can view the partition name to which the device group belongs, for example, "Partition1: Edge Routers" and "Partition2: Edge Routers". Refer to "Partitions" on page 158 for information on configuring partitions.

To view detailed information about a device group:

1. On the menu bar under Devices, click Groups. The Device Groups page opens.
2. Click the group name on which to view detailed information. The Device Group Details page opens.

Device Group Details Page Fields

Field	Description/Action
Groups link	Opens the Device Groups page, where you can view all of the device groups. Refer to "Device Groups Page Fields" on page 147 for information.
New Device link	Opens the New Device page where you can add a new device. Refer to "Adding Devices" on page 108 for information.
New Device Group link	Opens the New Group page, where you can add a new group. Refer to "Adding Device Groups" on page 138 for information.
New Parent Group link	Opens the New Parent Group page, where you can add a new parent group. Refer to "Adding Parent Groups" on page 140 for information.
Edit Group link	Opens the Edit Group page, where you can edit the device group. Refer to "Edit Group Page Fields" on page 162 for information.
Update Device List link	Refreshes the page and recalculates the device group membership.
Current Working Group	Shows the current working group in the drop-down menu. You can select a different group from the drop-down menu.
List Active Devices Only check box	If checked, the list of devices is restricted to actively managed devices.
Run Task on this Group	You can select a task from the drop-down menu to run on this group. Refer to "What Are Tasks?" on page 279 for information on running tasks.
Check Boxes	You can use the left-side check boxes to manage devices. Once you have selected the devices, click the Actions drop-down menu. Options include: • Activate — Instructs NA to manage the selected devices. • Deactivate — Instructs NA not to manage the selected devices. • Batch Edit — Opens the Batch Edit Device page, where you can assign a driver and set the connection methods for all the checked devices at once. Refer to "Batch Edit Device Page Fields" on page 163 for information. • Diagram — Opens the Diagramming page. Refer to "Diagramming" on page 609. • Delete — Deletes the selected devices. • Select a task to run against the device group. The adjacent Select drop-down menu enables you to select or deselect all of the devices.
Host Name	Displays the host name of the device. Clicking a host name opens the Device Detail page, where you can view information about the device and its configuration history.
Device IP	Displays the IP address of the device. Devices in red failed their most recent snapshot attempt. Inactive devices are marked with an icon beside the IP address. Clicking an IP address opens the Device Detail page, where you can view information about the device and its configuration history.
Device Vendor	Displays the name of the device manufacturer.
Device Model	Displays the model designation of the device.

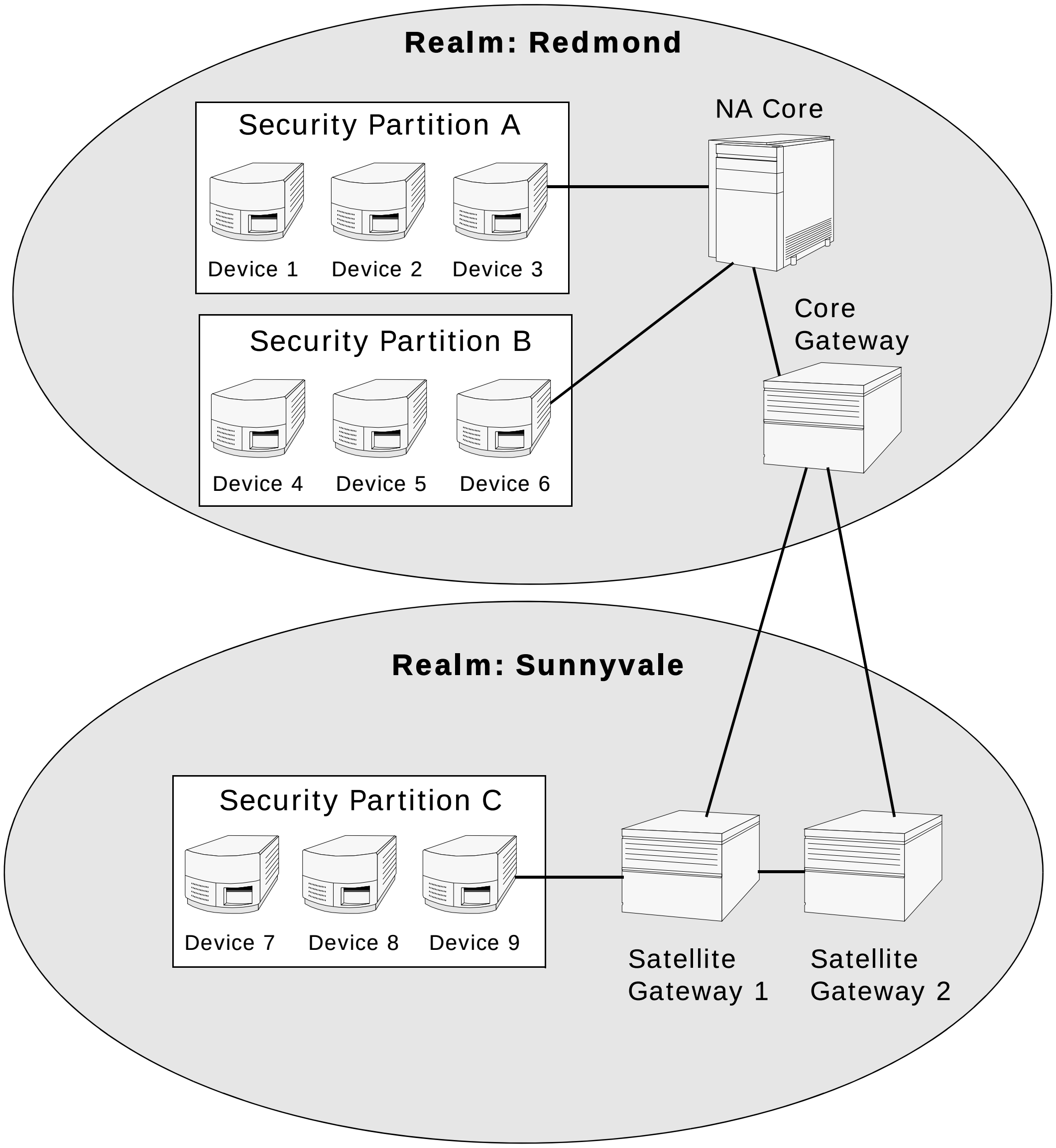
Field	Description/Action
Partition	Displays the Partition to which the device belongs. (**Note**: This field is only displayed if you have configured one or more Partitions.
Last Changed Time	Displays the date and time the device's configuration was last changed.
Actions	You can select the following actions: • Edit — Opens the Edit Device page, where you can edit the information for this device. Refer to "Edit Device Page Fields" on page 113 for information. • Telnet — Opens a Telnet window. • SSH — Opens an SSH Window. • View Config — Opens the Current Configuration page, where you can view the latest configuration and add comments.

Segmenting Devices and Users

NA provides the ability to manage overlapping IP networks and partition both devices (and device groups) and users (and user groups). The following terms are used in this section.

- **NA Core** — A single NA Management Engine, associated services (Syslog and TFTP), and a single database. A NA Core can manage multiple Partitions (set of devices). Multiple NA Cores can be connected in a Distributed System configuration. (For detailed information on installing and configuring a Distributed System, see the *NA Multimaster Distributed System on Oracle Guide* or the *NA Multimaster Distributed System on SQL Server Guide*.)
- **Security Partition** — A set of NA objects that are part of a Partition. NA objects can include devices, users, command scripts, device password rules, policies, software images, and so on. Partitions can be used in conjunction with a permissions model, group hierarchy, distribution of devices across NA Cores, and network diagramming.
- **Default Site Partition** — The default Partition (named Default Site). If you are new to NA, the default Partition is the only Partition available. The default Site Partition is needed by the system to connect to devices via the Gateway Mesh. It includes all of the devices currently managed by NA. You can rename the default Site Partition, however you cannot modify the properties. (**Note**: If you have configured multiple Partitions in earlier versions of NA, you will be able to edit those Partitions. However, you will not be able to add or delete Partitions.
- **Realm** — A network segment. In general, a Realm is identified by a set of unique IP addresses. For example, a Realm cannot contain two devices numbered as 10.255.111.128. Instead, the devices must be broken out into separate Realms. A Partition is not required to be in the same Realm as its managing NA Core. Keep in mind that a Realm is a large area that can include many Partitions. While a Realm does not have to include any NA Cores, typically a NA Core manages devices in its local Realm. A NA Core can manage devices in remote Realms via the Gateway Mesh.The Gateway Mesh is used to proxy IP traffic between Realms.

The following figure illustrates the various components of a multi-Security Partition configuration. Keep in mind that Realms and Partitions cannot overlap and a device cannot be in more than one Realm, as shown in the figure. However, there can be multiple Partitions and NA Cores in a Realm. There can also be multiple Gateways in a Realm.


Realm: Redmond
Security Partition A
Device 1
Device 2
Device 3
NA Core
Security Partition B
Device 4
Device 5
Device 6
Core Gateway
Realm: Sunnyvale
Security Partition C
Device 7
Device 8
Device 9
Satellite Gateway 1
Satellite Gateway 2

Local Realms

If a device is in a Local Realm, NA will connect directly to it without going through the NA Gateway Mesh.

When NA connects to a device, if the device is in the same Realm as the local Core, NA connects directly to the device. Otherwise, NA connects to the device through the Gateway Mesh by connecting to the local Core Gateway and requesting the Core Gateway to connect to the device in the specified Realm.

Note: Local Realms are aliases for the Core Realm. If a device is in the core Realm or in a local Realm, NA connects directly to the device.

Local Realms and NAT Access

If a NAT IP Address is assigned to a device in NA, NA connects to the device using the NAT IP Address. The NAT IP Address has a Realm associated with it, so the same rule applies. If the NAT IP Address Realm is local (either the core's Realm or a defined local Realm), access is direct. Otherwise, access is through the Gateway Mesh.

While NA could assume that all NAT access is local, allowing a Realm to be associated with a NAT IP address ensures that NA L3 network diagrams can correctly reflect that one interface on a device is in a different L3 cloud.

Local Realms and Console access

If a Console Server is defined for a device in NA, NA connects using the Console Server. The Console Server's IP Address also has a Realm name associated with it. It is handled the same as NAT access above.

Local Realms and Bastion Host Access

If a Bastion Host is defined for a device, NA uses the Bastion Host. You cannot assign a Realm to the Bastion Host IP address. NA always accesses the Bastion Host locally. This enables you to use local Realms to manage devices in different remote Realms without using the Gateway Mesh if there is Bastion Host access to the remote devices. Bastion Host access only allows CLI access to devices. As a result, SNMP and TFTP cannot be used. Since TFTP cannot be used, software updates will not work for devices using Bastion Host access.

Adding a Local Realm

To add a local Realm,

1. Edit the *$HPNA/jre/adjustable_options.rcx* file where $HPNA is the root of the NA installation (typically C:\Rendition on Windows).
2. Remove the comments around gateway/mesh/local_realms and add the local realm names:

```
<!--Gateway Mesh: define realms that do not use the Gateway Mesh-->
<array name="gateway/mesh/local_realms">
   <value>Local Realm 1</value>
   <value>Local Realm 2</value>
</array>
```

3. Restart NA.

Overlapping IP Networks

Every Partition must have a managing NA Core. However as shown in the previous figure, the managing NA Core does not have to be in the same Realm as the Partition it is managing.

When accessing devices, if the NA Core is in the same Realm, for example Device 3, NA directly connects to the device to manage it. If the NA Core is in a different Realm than a device it is managing, for example Device 9, NA connects to Satellite Gateway 1 in its Realm, which then communicates through the other Gateways to Device 9.

The collection of Gateways is called a *Gateway Mesh*. A Gateway in the same Realm as a NA Core is called a *Core Gateway*. A Gateway in a Realm without a NA Core is called a *Satellite Gateway*. The Gateway Mesh enables a NA Core to manage devices in different Realms. (Refer to “Device Access Page Fields” on page 47 for information on configuring the Gateway Mesh.)

Keep in mind that installing and configuring a HP Gateway is only required if you want to manage devices and networks that use duplicate and/or overlapping IP addresses. The HP Gateway is a standalone product and not bundled with NA.

You can configure multiple:

- Realms — Enables you to use overlapping IP addresses. That is, more than one device with the same IP address.
- Security Partitions (in the same Realm) — Enables you to restrict view access for users to devices that are in the same Realm. If a Partition is deleted, all objects are automatically placed in the Default Partition (named Default Site).
- Gateways (in the same Realm)— Enables you to improve up-time in the event that one Gateway fails.
- NA Cores (in the same Realm) — Enables you to share access to device information in the NA system. The NA Distributed System on Oracle is a multimaster system where data from each NA Core in a Gateway Mesh is accessible to all other NA Cores. This allows for redundant data and failover in the event of a NA Core crash. (For more information, see the *NA Multimaster Distributed System on Oracle Guide*.)

Setting Up The HP Gateway

The following terms are used in this section:

- **Gateway** — An application that routes IP traffic to other Gateways.
- **Gateway Mesh** — A collection of Gateways that route traffic between themselves.
- **Core Gateway** — A Gateway running in the same Realm with a NA Core.
- **Satellite Gateway** — A Gateway running in a Realm that does not have a NA Core.
- **IP Space** — One or more Realms that have no overlapping IP addresses.

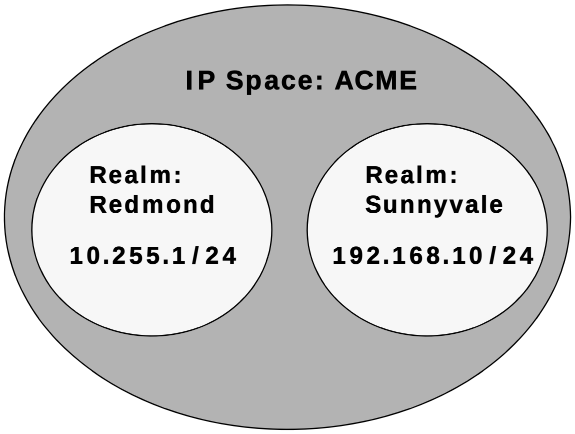
Using the HP Gateway with NA provides support for overlapping IP addresses (i.e., multiple devices that have the same IP address). In addition, by installing a NA remote agent on the same LAN with the devices being managed, Syslog and TFTP can be used to manage the devices locally. Refer to “Deploy Remote Agent Page Fields” on page 382 for information.

Note: If there are many NA users in the same LAN, a NA Core (NA Multimaster Distributed System) might be preferable to a NA remote agent on that LAN. For more information, see the *NA Multimaster Distributed System on Oracle Guide*.

In general, the HP Gateway enables a NA Core to manage servers that are behind one or more NATed devices or firewalls. It does this by creating persistent TCP tunnels between Gateway instances, much like SSH tunnels. In addition, the HP Gateway provides bandwidth management. This is important when a tunnel is transmitting over a low-bandwidth link and you need to limit usage of the bandwidth to a fixed amount that is less than the maximum link speed.

Note: For information on installing a Satellite configuration, see the *NA Satellite Guide*.

HP Server Automation (HP SA) uses the Gateway Mesh in each install. However, NA only uses the Gateway Mesh when needed to handle overlapping IP spaces. With NA/HP SA integration, a Realm can be a collection of networks with no overlapping IP addresses, as shown below. As a result, an IP Space can be defined as one or more Realms with no overlapping IP addresses.



NA Cores can be in different IP spaces in a NATed environment. If there is a NA Core in the same IP space, it is more efficient for the NA Core to communicate directly to devices instead of going through the Gateway Mesh, unless the NA Core is not topologically close to the devices being managed. To reduce WAN utilization, it might be beneficial to place a NA Satellite topologically close to the devices being managed.

To setup the HP Gateway, you need to install:

1. A Core Gateway for each NA Core
2. A Satellite Gateway for each remote Realm

Note: When sharing a Gateway between HP SA and NA, you must use the HP SA installer. The NA Gateway installer cannot install a Gateway that is used by HP SA. The NA Gateway installer is for NA-only Gateway Meshes.

For step-by-step instructions for installing a Core Gateway, installing a Satellite Gateway, and configuring NA to use the Gateway Mesh, see the *NA Satellite Guide*. Refer to "Device Access Page Fields" on page 47 for information on configuring the Gateway Mesh.

Gateway List Page Fields

The Gateway List page displays the currently configured Gateways and enables you to edit Gateway information. Refer to "Edit Gateway Page Fields" on page 157 for information.

To open the Gateway List page, on the menu bar under Admin, click Gateways. The Gateway List page opens.

Note: Once you have installed the Gateway Mesh, you need to install a NA remote agent on each Satellite Gateway host. Do not install a NA remote agent to the host with the Core Gateway.

Field	Description/Action
Deploy Remote Agent link	Opens the Deploy Remote Agent page, where you can deploy a NA remote agent. Refer to "Deploy Remote Agent Page Fields" on page 382 for information.
Monitor Satellite link	Opens the Monitor Details page, where you view monitor status.
IP Space	Displays the IP space name. An IP space is one or more Realms that have no overlapping IP addresses.
Realm	Displays the Realm name. The Realm name is returned from the Gateway. The Realm name is set when the Gateway is installed and cannot be modified in NA. To change the Realm name, you need to re-install the Gateway. (For instructions, see the *NA Satellite Guide*.)
Gateway	Displays the Gateway name. The Gateway name is set when the Gateway is installed and cannot be modified in NA. (For instructions, see the *NA Satellite Guide*.)
Host	Displays the hostname or IP address of the system on which the Gateway is installed. If the Gateway host has multiple IP addresses, this is the IP address that would be used from the Gateway host. The Host IP address is only important if you have more than one Gateway installed in the same Realm. **Note**: You can install multiple Satellite Gateways in the same Realm for redundancy.
Partition	Displays the Partition name associated with the Realm name, if applicable. Refer to the "Partitions" on page 158 for information.

Field	Description/Action
Core	In a Multimaster Distributed System environment, the Core name is set on the Edit Core page. If the Realm name on the Edit Core page matches the Realm name for a Gateway, the Gateway List page displays the Core name of the Core. For information on the Edit Core page, see the *NA Multimaster Distributed System on Oracle Guide*.
Agent	Displays the name of the NA remote agent for Satellite Gateways. The NA remote agent name can be changed on the Edit Gateway page. Once you have installed the Gateway Mesh, you must install a NA remote agent on each Satellite Gateway host. If there is no NA remote agents installed, the Agent column is empty. Refer to "Deploy Remote Agent Page Fields" on page 382 for information.
Actions	There is one option: • Edit — Opens the Edit Gateway page. Refer to "Edit Gateway Page Fields" on page 157.

Edit Gateway Page Fields

NA automatically sets the IP Space name based on the Realm Name. However, if two Realms are in the same IP Space, and you want them diagrammed correctly in L3 diagrams, you can edit the Gateway to set the IP Space name.

To open the Edit Gateway page, on the Gateway List page, click the Edit option in the Actions column.

Field	Description/Action
Gateway	Displays the Gateway name. The Gateway name is set when the Gateway is installed and cannot be modified in NA.
Realm	Displays the Realm name. The Realm name is returned from the Gateway. The Realm name is set when the Gateway is installed and cannot be modified in NA.
IP Space	Displays the IP space name. An IP space is one or more Realms that have no overlapping IP addresses. Enter a new IP space name.
Host	Displays the hostname or IP address of the system on which the Gateway is installed. Enter a new host name or IP address.
Satellite	Displays the Satellite Gateway running in a Realm that does not have a NA Core. Enter a Satellite Gateway name, if applicable.

Partitions

Partitions are a set of NA objects. NA objects can include devices, users, command scripts, device password rules, policies, software images, and so on. Partitions can also be used in conjunction with a permissions model, group hierarchy, distribution of devices across NA Cores, and network diagramming.

Partitions are always public groups. They can be placed within the device group hierarchy. If an object (i.e., Device, Device Group, User, or User Group) is added to Partition, it is automatically removed from the Partition to which it previously belonged.

If a Partition is deleted, all objects are automatically placed in the Default Partition (named Default Site). This is done to ensure that any device appears in only one Partition. Any reference to an IP address without an explicit Partition uses the default Partition. (Refer to "Segmenting Devices and Users" on page 150 for detailed information on Partitions.)

NA provides the ability to restrict which users can view other users. As a result, you can partition users and user groups in the NA system. For example, if a Managed Service Provider is managing a large banking institution, the users working for the Manager Service Provider can be rendered invisible to the bank's users. Keep in mind that when partitioning user objects, such as password rules, only users that have access rights to all Partitions can create and/or edit global (or shared) objects.

Partitions Page Fields

To open the Partitions page, on the menu bar under Admin click Security Partitions. The Partitions Page opens.

Field	Description/Action
Partition By	Select a Partition from the drop-down menu, if applicable. The default partition is named Site. The default Site Partition is needed by the system to connect to devices via the Gateway Mesh. Any reference to an IP address without an explicit Partition uses the default Site Partition.
Rename link	Enables you to rename the Partition. This name is displayed on the New Device, New Device Group, and New Parent Device Group pages. Refer to "New Device Page Fields" on page 108 for information.
New Partition link	Opens the New Partition page where you can create a new Partition. Refer to "New Partitions Page" on page 159 for information.
Partition Name	Displays the default Site Partition and any other Partitions that you have created.
Core	In a distributed NA installation, this specifies which NA Core will be used to manage devices in this Partition. **Note**: This option is not displayed if there is only one NA Core. (For more information, see the *NA Horizontal Scalability Guide*, the *NA Multimaster Distributed System on Oracle Guide*, or the *NA Multimaster Distributed System on SQL Server Guide*.)
Realm Name	Select a Realm from the drop-down menu. This specifies what Realm the devices and/or users in this Partition are in. **Note**: This option is not displayed if there is only one Realm (i.e., no HP Gateway Mesh). If the NA Core is not in the same Realm, NA uses the HP Gateway Mesh to connect to the devices in this Partition.

Field	Description/Action
Description	Provides a description of the Partition.
Number of Devices	Displays the number of devices in the Partition.
Actions	You can select the following actions: • Edit — Opens the Edit Partition page. Refer to "Edit Partition Page Fields" on page 159 for information. • Delete — Enables you to delete a Partition. Keep in mind that you cannot delete the default Site Partition.

New Partitions Page

To add a new Partition:

1. On the menu bar under Admin, click Security Partitions. The Partitions page opens.
2. Click the New Partition link at the top of the page. The New Partition page opens.
3. Enter the Partition name and a description.
4. In the Devices field, use the Device Selector to select the devices you want in the Partition. For information on how to use the Device Selector, refer "Device Selector" on page 144.

   Note: A Partition can apply to both devices and users. If the Partition applies to users, on the Edit User page you have the option of editing the Partition.

5. Click the Save button. The Partitions page opens displaying the current Partitions. Keep in mind there is one default Partition named *Default Site*. This Partition contains all of the discovered devices in your network.

Edit Partition Page Fields

To edit a Partition:

1. On the menu bar under Admin, click Security Partitions. The Partitions page opens.
2. For the Partition you want to edit, click the Edit option in the Actions column. The Edit Partition <name> page opens. The following table includes the fields when editing the default Site Partition.

Field	Description/Action
Partition Name	Displays the Partition name.
Description	Provides a description of the partition.
Core	This field is only displayed for partitions in the default Partition. In a distributed NA installation, this specifies which NA Core will be used to manage devices in this Partition. (Refer to "Overlapping IP Networks" on page 153 for more information on NA Cores.)

Field	Description/Action
Realm Name	This field is only displayed for Partitions in the default Site Partition. Select a Realm from the drop-down menu. This specifies what Realm the devices in this Partition are in. If the NA Core is not in the same Realm, NA uses the Gateway Mesh to connect to the devices in this Partition.
Devices	A list of devices is displayed in the Device Selector's Devices box. For information on how to use the Device Selector, refer to "Device Selector" on page 144. Keep in mind that when you add a device to a partition, it is automatically removed from its previous partition. In addition, to delete a partition, you must move all the devices from it into a different partition before the system can delete it.

Be sure to click the Save button when you are done.

Adding Devices to a Partition

To add devices to a Partition:

1. On the menu bar under Admin click Security Partitions. The Partitions page opens.
2. In the Partition Name column, click the Partition you want to edit. The Partition page opens. This page is similar to the Inventory page, where you can view a list of the managed devices in the Partition. However, there are two added links at the top of the page: Edit Group and Partitions. Clicking the Partitions link returns you to the Partitions page. (Refer to "Inventory Page Fields" on page 188 for information.)
3. Click the Edit Group link to open the Edit Partition page, where you can edit the devices in the Partition. Be sure to click the Save button when you are finished. (Refer to "Segmenting Devices and Users" on page 150 for detailed information on Partitions.)

Field	Description/Action
Partition Name	Displays the name of the Partition.
Description	Displays the description of the Partition.
Devices	A list of devices is displayed, if applicable. For information on how to use the Device Selector, refer to "Device Selector" on page 144.

Be sure to click the Save button when you are done.

Viewing Partition Details

A Partition can be a set of devices and/or users. A device and/or user can only be in one partition. If there is more than one Partition, each device and/or user is in one (and only one) Partition.

To view and/or edit Partition information:

1. On the menu bar under Admin click Security Partitions.
2. Click the Partition of which you want information. Refer to "Inventory Page Fields" on page 188 for information.

Editing Device Groups

To edit an existing device group:

1. On the menu bar under Devices, click Groups. The Device Groups page opens.
2. Click Edit in the Actions column for the device group you want to edit. The Edit Group page opens. Be sure to click Save when you are done.

Edit Group Page Fields

Field	Description/Action
Group Name	Displays the name of the device group.
Description	Displays a description of the device group.
Partition	Select a Partition from the drop-down menu. (**Note**: This field is only displayed if you have configured one or more Partitions.) In general, a Partition is a grouping of devices with unique IP addresses. Multiple Partitions can be managed by a single NA Core. A NA Core is an installation of a NA server, comprised of a single Management Engine, associated services, and a single database.
Sharing	Either informs you that the device group you are editing is public or private, or that the device group is a parent group. If you are editing a leaf group, you are informed that the device group has a parent.
Parent Device Group	Displays the name of the parent device group in the drop-down menu.
Devices	Select one of the following options: • Use Device Selector to select a fixed device group (static group) — For information on how to use the Device Selector, refer to "Device Selector" on page 144. • Use filters to define a dynamic device set (dynamic group) — The display changes, enabling you to configure searches using one or more search criteria, create a Boolean expression using the AND and OR operators to filter searches, or limit a search by device group. **Note**: This tool does not support the use of regular expresssions.
Child Device Groups	• All device groups — Displays a list of all current device groups. Select the device groups you want to include as children of the parent group and click Copy >>. • Children of this group — Displays a list of device groups that are assigned to the parent group as children. Select the child groups you want to remove from this parent group and click << Remove.

Editing a Batch of Devices

The batch edit functionality enables you to make changes to device settings. You can:

- Assign a driver
- Set connection methods (SNMP, SNMPv3, Telnet, SSH)
- Set transfer protocols (SCP, TFTP, FTP)
- Set bastion host information
- Reset the last used password
- Set ACL parsing

1. On the menu bar under Devices, click Inventory. A list of all currently managed devices opens.
2. Check the check boxes for the devices you want to edit in one batch operation.
3. On the Actions drop-down menu, click Batch Edit. The Batch Edit Device page opens. Be sure to click the Save button when you are finished.

Batch Edit Device Page Fields

Field	Description/Action
Devices	Lists the selected devices.
Assign Driver	If checked, select the driver to assign to the batch of devices.
Set Connection Methods	If checked, select the access methods for the batch edit from the following connection methods and transfer protocols: Connection Methods: • SNMP • SNMPv3 (user authentication) — With SNMPv3, you have the following options: noAuthNoPriv (username only), authNoPriv (username, authentication password), and authPriv (username, authentication. and encryption password). Authentication methods include SHA (Secure Hash Algorithm) and MD5 (Message Digest Algorithm). Encryption methods include DES (Data Encryption Standard), AES (Advanced Encryption Standard), AES192, and AES256. • SNMPv1 or SNMPv2c (checked by default) • Telnet • SSH — Select either SSH1 or SSH2 (the default), SSH1 Only, or SSH2 Only. Transfer Protocols (checked by default): • SCP • SFTP • FTP • TFTP

Field	Description/Action
Set Bastion Host Information	If checked, enter the following information: • Use a Unix or Linux bastion host for Telnet and SSH access, if applicable • IP address or Host Name of the bastion host • Bastion Host Username • Bastion Host Password • Confirm the password
Reset Last Used Passwords	If checked, reset last used passwords.
Set ACL Parsing	If checked, select one of the following options: • Enable ACL parsing and storage with each snapshot. • Disable ACL parsing and storage with each snapshot.
Set Hierarchy Layer	Select a Hierarchy Layer from the drop-down menu.
Set Custom Service Type	If checked, select a service type. Service types can specify VoIP, BGP, MPLS, and so on. The values help to identify the device's purpose. You can use these values to tag device services so as to easily search for them or view them in a group (static or dynamic).
Set Custom Data Field	If checked, you can edit the custom data you assigned to a device. Refer to "Enhanced Custom Fields Setup" on page 564 for information.

Discovering Device Drivers

Discovery matches an appropriate device driver to any device. The device driver translates proprietary commands for each device to the universal format that NA uses to manage heterogeneous networks.

Discovery queries each new device using SNMP or Telnet/SSH and assigns the appropriate device driver. If this process fails, the result appears on the Recent Tasks page. NA cannot actively manage a device configuration until the correct driver is assigned. If driver discovery fails, you can assign a driver manually. Refer to the Driver Release Service (DRS) documentation for detailed information on supported devices. The DRS is an automated driver release and delivery system.

To initiate the device driver discovery process, on the menu bar under Devices, select New Device Task and click Discover Driver. The New Task - Discover Driver page opens. Refer to "Discover Driver Task Page Fields" on page 295. Keep in mind that device driver discovery is also initiated by the Deploy Software task. After software is successfully uploaded (and the device is rebooted, if this option is selected), a device driver discovery task is initiated.

Accessing Devices Using Telnet

Launching Telnet and SSH sessions from NA offers several benefits:

- Simplify logins — Users login using their NA account. NA verifies the user's permissions. The user can enter NA CLI commands or connect directly to a device. The user can exit from one device, then connect to another, and so on, in one session. The user must remember only one login, regardless of device vendors, types, and so on. If the requested login method does not work, NA automatically tries backup login methods.
- Organize by groups and permissions — Organizing devices into groups and assigning permissions per group ensures that users access just the devices they care about and have permissions for.
- Store configurations, even without AAA — The Telnet/SSH Proxy enables you to store modified configurations, in-line comments, and who made changes. The Telnet/SSH Proxy automatically associates audit logs of sessions to the configurations.
- Reduce ACLs — You need an Access Control List (ACL) only for the NA server, rather than one ACL per device.
- Increase security — Identifying who is changing devices on your network makes it easier to detect an unauthorized user and track unauthorized changes. NA also makes it easy to deploy a stable configuration stored prior to the unauthorized changes, correcting potential damage and restoring network service quickly.

In addition, you can connect your Telnet/SSH client to devices through NA, and track the sessions. NA has been tested with connections from the following clients (though others may also work):

- SecureCRT
- Windows Telnet
- Putty

There are a number of Admin Settings related to the Telnet/SSH Proxy interface. Refer to "Telnet/SSH" on page 67 for information.

To initiate a Telnet session using NA, on the menu bar under Devices, click Inventory. A list of all currently managed devices opens. Select the Telnet option in the Actions column for the device. You are logged into the device and you see the device prompt in the Telnet window.

Note: If your system does not already have the Java Runtime Environment (JRE) installed, your browser initiates a download from the Sun Website the first time you use Telnet or SSH. This is expected and you should approve the download and installation of the JRE.

The first time you run a Telnet or SSH session from NA, you may see a security window asking you to download a certificate from HP. Click Grant always to continue. This verifies that you trust content from HP.

You can enter whatever device commands you like. Enter *quit* when finished. This logs you out of the Telnet session, but you remain in a NA Telnet Proxy session. The Proxy session uses the `NA>` prompt.

In a Telnet/SSH Proxy session, you can connect to another device or enter NA CLI commands. You can initiate a Proxy session directly by clicking Connect at the top of any page.

Note: Although NA will attempt to separate all command/response sequences from the session, this is not foolproof. When a device automatically completes a command, or when the device prompts for further command parameters, the result in not necessarily a clear command/response separation. In addition, a session that includes the use of these kinds of interactive shortcuts might not be a good candidate for the generation of an advanced script.

Accessing Devices Using SSH

To initiate an SSH session, on the menu bar under Devices, click Inventory. A list of all currently managed devices opens. Select the SSH option in the Actions column for the device. You can enter whatever device commands you like. Enter *quit* when you are finished.

Note: You can initiate a Proxy session directly by clicking Connect at the top of any page. In a SSH Proxy session, you can connect to another device or enter NA CLI commands.

Listing Telnet/SSH Sessions

To list Telnet and SSH sessions, on the menu bar under Devices, click Inventory. A list of all currently managed devices opens. Click the device. The Device Details page for that device opens. From the View drop-down menu, click Telnet/SSH Sessions. The Telnet/SSH Session page opens with the device host name or IP address at the top.

Telnet/SSH Session List Page Fields

Field	Description/Action
Check Boxes	You can use the left-side check boxes to delete sessions. Once you have selected the session, click the Actions drop-down menu and click Delete. The adjacent Select drop-down menu enables you to select or deselect all sessions.
Start Date	Displays the date and time the session began.
Status	Displays the status of the session, either Open or Closed.
Type	Displays the type of session, either Telnet or SSH.
End Date	Displays the date and time the session ended.
Created By	Displays the name of the person who created the session.
<Custom Fields>	All custom fields defined for Telnet/SSH sessions appear on this page.
Actions	You can select from the following options: • View Full Telnet/SSH Session — Opens the Telnet/SSH Session page, where you can view the commands entered and the device responses during this session. • View Commands Only — Opens the Telnet/SSH Session page, where you can view only the commands entered during this session. This is useful for recording scripts to replay on this or other devices. Click any command to view the device response to that command.

Note: Selecting text with the left mouse button highlights the text. You can then press the Enter key to paste the text onto the clipboard. Pressing the right mouse button inside the Telnet/SSH applet pastes the text from the clipboard to the applet.

A shortcut when using connect is adding wildcards to the host name or IP address, such as `connect dev*`. This returns a list of devices (or a message to narrow your search). Enter the number of the device you want to connect to. The Shell interface supports the following control characters.

Control Character	Description
^A	Moves the cursor to beginning of the input line.
^B, Left Arrow	Moves the cursor back one character.
^C	Cancels the input line and returns a new prompt.
^D	Erases the character under the cursor.
^F, Right Arrow	Moves the cursor right one character.
^H, Backspace, Delete	Erases the character to the left of the cursor.
^J, ^M	Sends a CRLF.
^K	Kills from the cursor to end of line and places text in the kill buffer.
^L, ^R	Echoes a command on new command line (simulates screen redraw).
^N, Down Arrow	Moves to the next command in the command history.
^P, Up Arrow	Moves to the previous command in the command history.
^T	Transposes the character under the cursor with the previous character.
^U, ^X	Deletes from the cursor to the beginning of line, and places the deleted characters in the kill buffer.
^W	Deletes from the cursor to the beginning of word, and places the deleted characters in kill buffer.
^Y	Yanks from the kill buffer to the current location.
^\	Closes the current device connection (useful for access through a console server).
ESC-b	Moves the cursor backwards one word.
ESC-f	Moves the cursor forwards one word.

Making Configuration Changes Using The Telnet/SSH Proxy

Do the following to make configuration changes via the Telnet/SSH Proxy.

1. Telnet or SSH to the NA server and login using your NA credentials.
2. Use the *connect* command to connect to devices. You can enter `connect*` to view the devices available for connection through NA. If there are too many devices to display, narrow the field by entering the first few letters of the hostname (or digits of the IP address), followed by an asterisk, for example: `connect bor*`.
3. Enter the number from the list of numbers displayed in the Telnet/SSH Proxy of the device to which you want to connect. NA automatically logs you into the device after checking your access credentials.
4. Assuming that this is a Cisco IOS device, enter `Config T` mode on the device, make the change, and add any relevant comments.
5. Exit out of Configure Terminal mode and enter `Exit`.
6. To exit the NA Telnet/SSH Proxy, enter `Exit` at the prompt.

Keep in mind when using the Telnet/SSH Proxy, in-line commenting occurs as you are logged into the device.

Using a Bastion Host

A bastion host is a gateway between a private network and a public network. Used as a security measure, a bastion host can act as a barrier between private and public networks to prevent attacks by hackers.

Using a bastion host with NA enables you to have lockdown capability over Telnet or SSH access. You can:

- Specify a bastion host on a per device basis.
- Specify username (optional) and password as login credentials for the bastion host.
- Telnet or SSH to the bastion host and then Telnet or SSH through to the target device.

Note: When using a bastion host, all CLI access will be routed through the bastion host rather than directly to the device. When connecting via the Telnet/SSH Proxy to a device configured to use a bastion host, NA connects via the bastion host, and applies the user's AAA credentials, if indicated, to both the bastion host and the target device.

Keep in mind that access to a bastion host will not go through the normal NA password rules processing. If the bastion host credentials are invalid, there is no fallback. After logging into the bastion host, access from there to the device will follow the normal password processing in NA.

Note: Multiple bastion hosts cannot be specified for an specific device. However, you can simulate this by load-balancing across multiple bastion hosts that share a DNS name.

To designate a Unix or Linux bastion host for Telnet & SSH access:

1. On the menu bar under Devices, click Inventory. A list of all currently managed devices opens.
2. Click the New Device link at the top of the page. The New Device page opens.
3. Scroll down to the middle of the page to locate the Connection Information section. Refer to “New Device Page Fields” on page 108 for information.

To designate if new devices should use a bastion host by default for Telnet and SSH access, on the menu bar under Admin, select Administrative Settings and click Device Access. Refer to “Device Access Page Fields” on page 47 for information.

Chapter 4: Managing Device Configurations

Use the following table to quickly locate information.

Topic	Refer to:
Getting Started	"Getting Started" on page 174
Viewing Device Configuration Changes	"Viewing Device Configuration Changes" on page 174
Comparing Device Configurations	"Comparing Device Configurations" on page 181
Deploying Device Configurations	"Deploying Device Configurations" on page 182

Getting Started

HP Network Automation (NA) detects and records device configuration changes. When a device configuration change occurs, NA downloads the configuration into its centralized repository. NA supports multiple real-time change detection and alerting systems that enable you to immediately identify what changes were made and by whom.

For devices that support user attribution via Syslog, such as Cisco IOS devices, NA extracts the username and associates it with a configuration change. If NA cannot associate the username with an NA user, a new user account is created with a randomly generated password. By default, NA appends the term “_auto” to the new user to distinguish it as auto-generated. This enables NA to report ownership for all changes, including ones made by unregistered users. NA uses several methods, including AAA accounting logs, Syslog messages, and Proxy logs to discover the author of a given configuration change.

Access Control Lists (ACLs) are part of the configuration on many devices. They filter network traffic by controlling whether forwarded packets are accepted or blocked at the router's interfaces.

In general, the definition of an ACL is a collection of configuration statements. These statements define addresses, protocols, and patterns to accept or deny. ACLs can be used to restrict the contents of routing updates and to provide network security.

NA retrieves configuration information from devices and extracts the ACL statements and applications from the configuration. NA then stores the ACLs independent of the configuration. Refer to “Creating ACLs” on page 690 for detailed information on creating ACLs.

Viewing Device Configuration Changes

The Configuration Changes page enables you to view configurations that have changed. Devices that appear in red text failed a recent task. Inactive devices are indicated with an icon next to the IP address.

With configuration changes shown in different colors, you can easily scan two configurations and quickly identify the areas that have changed. Without NA to automatically identify a misconfigured device, you must manually connect to the device, call up the configuration, and identify if there is anything anomalous about it.

To view a complete list of all recent configuration changes, on the menu bar under Devices, click Configuration Changes. The Configuration Changes page opens. You can click a device to view specific device configuration information.

To view configuration changes for a specific device:

1. On the menu bar under Device, click Inventory. A list of all currently managed devices opens.
2. Click the device for which you want to view configuration changes. The Device Details page for that device opens.
3. From the View drop-down menu, click Configuration Changes. The Device Configurations page opens. For information on the Device Configuration Detail page, refer to “Device Configuration Detail Page Fields” on page 177.

Device Configurations Page Fields

Field	Description/Action
Hostname	Displays the device's host name. Clicking the device's host name opens the Device Details page, where you can view information about this device.
Device IP	Displays the device's IP address. Clicking the device's IP address opens the Device Details page, where you can view information about this device.
Last Snapshot Attempt	Displays the date and time the device was last accessed.
Last Snapshot Result	Displays the last snapshot result, for example "Configuration unchanged."
View menu	Refer to "View Menu Options" on page 203 for information.
Edit menu	Refer to "Edit Menu Options" on page 232 for information.
Provision menu	Refer to "Provision Menu Options" on page 241 for information.
Connect menu	Refer to "Connect Menu Options" on page 243 for information.
Scheduled Deployments for Device link	Opens the Task Search Results page, where you can view if there are any deployments scheduled for the device.
Edited Configurations link	Opens the Edited Configuration Search Results page. Refer to "Configuration Search Results Page Fields" on page 499 for information.
Check Boxes	You can use the left-side check boxes to compare two device configurations and/or delete device configurations. Once you have selected the devices, click the Actions drop-down menu and click either: • Compare — Opens the Compare Device Configurations page, where you can compare the two selected configurations side-by-side. The differences are highlighted in different colors to make them easy to view. • Delete — Deletes the checked device configurations. The adjacent Select drop-down menu enables you to select or deselect all of the device configurations.
Date	Displays the date and time the configuration was added or changed.
Changed By	Displays the login name of the person who changed the configuration, device, or task. N/A means not applicable.
Comments	Displays any comments about the configuration.

Field	Description/Action
Actions	You can select the following actions: • Compare to Previous — Opens the Compare Device Configuration page, where you can view the selected configuration and its previous configuration side-by-side. The differences are highlighted in different colors to make them easy to view. • View Config — Opens the Device Configuration Detail page, where you can view the entire configuration, deploy this version of the configuration to the device running configuration or startup configuration, and reboot, if applicable. You can also edit the configuration, download the text version of the configuration, email the configuration, and compare the configuration to the previous or next configuration. Refer to "Device Configuration Detail Page Fields" on page 177 detailed information. • Diagnostics — Opens the Diagnostics page, where you can view diagnostic information for this configuration. Diagnostics include Basic IP, Device Information, NA Detect Device Boot, NA Interfaces, NA Module Status, NA OSPF Neighbors, and NA Routing Table. For detailed information on diagnostics, refer to "View Menu Options" on page 203.

If the Startup and Running Configurations differ, the following links are displayed at the top of the Device Configurations page:

- View Startup — Opens the Device Configuration page, where you can view the current startup configuration. Refer to "Device Configuration Detail Page Fields" on page 177 for information.
- Compare Startup with Running — Opens the Compare Device Configurations page, where you can compare the Startup and Running Configurations. Refer to "Compare Device Configurations Page Fields" on page 181 for information.
- Synchronize — Opens the New Task - Synchronize Startup and Running page, where you can synchronize the Startup and Running Configurations. Refer to "Synchronize Startup and Running Task Page Fields" on page 321 for information.

Device Configuration Detail Page Fields

The Device Configuration Detail page enables you to:

- Examine the details of a particular configuration.
- Enter comments about the configuration.
- Deploy this version of the configuration to the device. For example, you could deploy a stable configuration to roll back an incorrect change to the device.

Note: For easy navigation, there are links directly above the configuration text that enable you to quickly parse sections of the configuration file. For example, if the configuration file includes an Access List section, you can click the Access List link at the top of the configuration file and navigate directly to that section. Note that currently, only the Cisco IOS generic driver supports section parsing.

To view the Device Configuration Details page for a specific device:

1. On the Device Details page, click the View drop-down menu and then click Configuration Changes. The Device Configurations page opens.
2. In the Actions column, click the View Config link option. The Device Configuration Detail page opens.

Field	Description/Action
Hostname	Displays the device’s host name. Clicking the device’s host name opens the Device Details page, where you can view information about this device.
Device IP	Displays the device’s IP address. Clicking the device’s IP address opens the Device Details page, where you can view information about this device.
Last Snapshot Attempt	Displays the date and time the device was last accessed.
Last Snapshot Result	Displays the last snapshot result, for example “Configuration unchanged.”

Field	Description/Action
Watch Device Link	If you click the Watch Device option for the first time, a Watch Group is created, along with a Watch Devices event rule, that includes the device. Any changes to the device will trigger an email notification for the user watching the device. The Watch Devices event rule will send an email notification for a variety of events, such as: • Device Access Failure • Device Booted • Device Configuration Change • Device Deleted • Device Diagnostic Changed • Device Edited • Device Software Change • Software Vulnerability Detected **Note**: You can edit the Watch Devices event rule to change events. All future watched devices will use the same event rule name. Refer to "New Event Notification & Response Rules Page Fields" on page 462. To remove a device from the Watch Group, click Stop Watching Device.
View menu	Refer to "View Menu Options" on page 203 for information.
Edit Menu	Refer to "Edit Menu Options" on page 232 for information.
Provision menu	Refer to "Provision Menu Options" on page 241 for information.
Connect menu	Refer to "Connect Menu Options" on page 243 for information.
Deploy to running configuration link	Opens the New Task - Deploy Config page, where you can deploy the configuration to the running config. (**Note**: This action may not be available for all devices.) Refer to "Deploy Config Task Page Fields" on page 183 for information.
Deploy to startup configuration and reboot link	Opens the New Task - Deploy Config page, where you can deploy the configuration to the startup config and reboot the device (so the startup and running configurations remain synchronized). (**Note**: This action may not be available for all devices.) Refer to "Deploy Config Task Page Fields" on page 183 for information.
Deploy Binary Configuration and Reboot link	Deploys the binary configuration to the device and reboots the device.
View Text Config link	Displays the configuration in plain text in a new browser window so you can copy it to the clipboard and paste it into other applications.
Download Text Config link	Downloads the configuration in Text format so you can copy it to another system.
Download Binary Config link	Downloads the configuration in Binary format so that you can copy it to another system.
Email Text Config link	Enables you to email the configuration.

Field	Description/Action
Compare to previous link	Opens the Compare Device Configurations page, where you can view the older and newer configurations side-by-side. The differences are highlighted in different colors to make them easy to view. **Note**: If this is the first configuration, the text will read, “This is the first configuration.” If this is the last configuration, the text will read, “This is the current configuration.”
Changed By	Displays the login name of the person whose change triggered the snapshot and a “Details” link so as to provide user details.
Create Date	Displays the date and time of the snapshot that captured the configuration change.
<custom fields>	Displays any custom fields defined for device snapshots and diagnostics.
Configuration Comments	Enter comments to differentiate this configuration from others, especially the previous configuration. Click Edit Comments. The Edit Comments option enables you to edit the custom fields and comments for this configuration. Refer to “Editing Device Configuration Data” on page 180 for information on editing device configuration data.
Line/Configuration Text	Displays the configuration file.

Editing Device Configuration Data

You can add or edit configuration comments by clicking the Edit Inline Configuration Comments option from the Edit menu. For information on adding custom data, refer to "Custom Data Setup Page Fields" on page 560.

When editing in-line comments:

- Whenever a line in a configuration changes, the comment for that line is removed. For example, if you change the host name, NA also removes any comment immediately above the host name command because NA cannot be sure the comment remains valid after the command is changed.
- Be careful when adding or removing blank lines. Because blank lines can be significant for some devices, NA treats added or removed blank lines as configuration changes. You can add blank comment lines (lines that begin with a double comment character, usually! or ##).
- In-line comments are not versioned in the same way as configuration files. A comment block applies to the next command in the configuration. If a deployment does not affect the next command line, the comment does not change. If you deploy an old configuration (to overwrite a new one), the comments from the newer configuration may be applied to the deployed configuration, even though the comments might end up in the wrong places.
- If you are concerned about losing comments in a file that requires significant editing, it is recommended that you copy the configuration file with the comments before saving, so you can restore comments if necessary.

Comparing Device Configurations

The Compare Device Configuration page displays two configurations for the same device side-by-side. Additions, deletions, and changes are highlighted in two columns with line numbers on the left. Each configuration is identified by its unique IP address and the date/time on which the configuration snapshot was taken.

To compare two configurations from different devices:

1. On the menu bar under Devices, click Configuration Changes. The Configuration Changes page opens.
2. Using the left-side check boxes, click any two devices.
3. On the Actions drop-down menu, click Compare. The Compare Device Configurations page opens.

Compare Device Configurations Page Fields

Field	Description/Action
Lines Changed	Displays the number of lines changed, highlighted in light purple.
Lines Inserted	Displays the number of inserted lines, highlighted in light green.
Lines Deleted	Displays the number of lines deleted, highlighted in light yellow.
Show differences with context	If selected (the default), only changes with three lines before and after each change are displayed.
Show full text	If checked, the complete configuration file is displayed.
Show UNIX-style diff	If checked, the configuration file is displayed in UNIX diff format.
Deploy to Running configuration link	Opens the Deploy Configuration page, where you can deploy this configuration to the running config on the device. (**Note**: This action may not be available for all devices.)
Deploy to startup configuration and reboot	Opens the Deploy Configuration page, where you can deploy the configuration to the startup config and reboot the device (so the startup and running configurations remain synchronized). (**Note**: This action may not be available for all devices.)
Configuration #1/ Configuration #2	Clicking the Configuration #1 or Configuration #2 link opens the Device Configuration Detail page. Refer to "Device Configuration Detail Page Fields" on page 177 for information. **Note**: If this is the first configuration, the text will read, "This is the first configuration." If this is the last configuration, the text will read, "This is the current configuration."
Device	Displays the host name and IP address for the device. Clicking the device's host name and IP address opens the Device Details page, where you can view information about this device and its configuration history.
Date	Displays the date and time of the snapshot that captured the configuration change.

Deploying Device Configurations

There are two ways to deploy a configuration:

- To the running configuration — When deployed, the configuration file remains in use until the device is rebooted. Rebooting the device might cause the startup configuration to overwrite the running configuration.
- To the startup configuration — When deployed, the device is rebooted and the new configuration becomes both the running and startup configuration.

To deploy a configuration:

1. On the menu bar under Devices, click Configuration Changes. The Configuration Changes page opens.
2. In the Actions column for a device, click View Config. The Device Configuration Detail page opens. Select one of the following options (if applicable):
   - Deploy to running configuration — Opens the New Task - Deploy Config page, where you can deploy this configuration to the running config on the device.
   - Deploy to startup configuration and reboot — Opens the New Task - Deploy Config page, where you can deploy the configuration to the startup config and reboot the device (so the startup and running configurations remain synchronized).

Deploy Config Task Page Fields

Field	Description/Action
Task Name	Displays Deploy Config. You can enter a different task name if applicable.
Applies to	Displays the device's Host Name or IP address.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Priority	Displays the task's priority. There are five task priority levels, 1 through 5. 1 is the highest task priority level. Refer to "Scheduling Tasks" on page 280 for more information.
Comments	Enter comments about the task.
Task Options	
Session Log	To store the complete device session log, click the "Store complete device session log" check box. Keep in mind that most tasks that interact with a device can be run with session logging enabled. This provides a detailed log of the interaction with the device during the task. Session logs should be viewed as the first step to debugging device-specific issues. Session logs provide details on CLI, SNMP, and all transfer protocol actions taken during the task. (**Note**: Large amounts of data could be stored. Refer to "Logging" on page 98 for detailed information on logging.)
Force Save	The device configuration update setting. This setting applies to only those devices that support a startup configuration. The default value of this setting is configurable per task type. • If NA should overwrite the startup configuration with the current running configuration at the completion of this task, select the Force Save check box. • If NA should not change the startup configuration, clear the Force Save check box. (**Note**: This setting is new in NA 9.20. It overrides all other approaches to determining whether to update the device startup configuration.)
Check boxes	The "Verify that changes are compliant with all policies that apply to the device" option is checked by default. Depending on the task type, you can also opt to "Deploy to running configuration" or "Deploy to startup configuration and reboot."
Configuration	Displays the configuration.
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.

Field	Description/Action
Device Credentials Options Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Server page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to "Server Page Fields" on page 54 for information on enabling Device Credentials.)	
Device Credentials	Depending on the Device Credentials options enabled on the Server page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use task-specific credentials. You are prompted to enter Username, Password, Confirm Password, Enable Password, Confirm Enable Password, SNMP Read-Only Community String, and SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)
Pre-Task / Post-Task Snapshot Options Snapshot options only appear if the system is configured to enable user overrides on the Configuration Mgmt Page under Administrative Settings. (Refer to "Configuration Mgmt Page Fields" on page 38 for information.)	
Pre-Task Snapshot	Select one of the following options: • None (the default) • As part of task
Post-Task Snapshot	Select one of the following options: • None • As part of task (the default) • Scheduled as a separate task
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflow. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.

Field	Description/Action
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to “Logging” on page 98 for detailed information on logging.

Be sure to click Save Task when you are finished.

Chapter 5: Viewing Devices

Use the following table to quickly locate information.

Topic	Refer to:
Viewing Devices	"Viewing Devices" on page 188
Viewing Device Groups	"Viewing Device Groups" on page 190
Reserving Devices	"Reserving Devices" on page 192
Viewing Device Details	"Viewing Device Details" on page 195
NA/SA Integration	"NA/SA Integration" on page 198
View Menu Options	"View Menu Options" on page 203
Virtual Local Area Networks (VLANs)	"Virtual Local Area Networks (VLANs)" on page 215
Edit Menu Options	"Edit Menu Options" on page 232
Provision Menu Options	"Provision Menu Options" on page 241
Connect Menu Options	"Connect Menu Options" on page 243

Viewing Devices

To view a list of the managed devices, on the menu bar under Devices click Inventory. Inventory is the default working group. It lists all of the currently managed devices. Refer to “Adding Devices” on page 108 for information on adding new devices.

Inventory Page Fields

Field	Description/Action
Groups link	Opens the Device Groups page, where you can view a list of current device groups. Refer to “Viewing Device Groups” on page 190 for information.
New Device link	Opens the New Device page, where you can add a new device. Refer to “Adding Devices” on page 108 for information.
New Device Group link	Opens the New Device Group page, where you can add a new device group. Refer to “Adding Device Groups” on page 138 for information.
New Parent Group link	Opens the New Parent Group page, where you can add a new parent group. Refer to “Adding Parent Groups” on page 140 for information.
Current Working Group	Displays Inventory, the default group. You can select a different group from the drop-down menu, if applicable.
List active devices only check box	Check this box if you want the inventory list to include only active devices. Inactive devices are not actively managed.
Run Task on this Group	You can select a task from the drop-down menu to run on this group. Refer to “What Are Tasks?” on page 279 for information on running tasks.
Group Description	List of all devices known to the system.
Check Boxes	You can use the left-side check boxes to manage devices. Once you have selected devices, click the Actions drop-down menu. Options include: • Activate — Instructs NA to manage the selected devices. • Deactivate — Instructs NA not to manage the selected devices. • Batch Edit — Opens the Batch Edit Device page, where you can assign a driver and set the connection methods for all the selected devices at once. Refer to “Batch Edit Device Page Fields” on page 163 for information. • Diagram — Opens the Diagramming page. Refer to “Diagramming” on page 609. • Delete — Deletes the selected devices. • Select a task to run against the checked devices. Refer to “Running Tasks Against Ad-hoc Device Groups” on page 279 for information. The adjacent Select drop-down menu enables you to select or deselect all of the devices.
Host Name	Displays the host name of the device. Devices in red failed the last snapshot attempt. Inactive devices are marked with an icon beside the IP address. Clicking the Host Name link opens the Device Details page, where you can view basic information about the device and its configuration history. Refer to “View Menu Options” on page 203 for information on the Device Details page.

Field	Description/Action
Device IP	Displays the IP address of the device. Clicking the Device IP link opens the Device Details page, where you can view basic information about the device and its configuration history. Refer to “View Menu Options” on page 203 for information on the Device Details page.
Device Vendor	Displays the device manufacturer’s name.
Device Model	Displays the device’s model designation.
Partition	Displays the Partition to which the device belongs. (**Note**: This field is only displayed if you have configured one or more Partitions.
Actions	You can select the following actions for each device: • Edit — Opens the Edit Device page, where you can edit the information for this device. Refer to “Edit Device Page Fields” on page 113. • Telnet — Opens a Telnet window. • SSH — Opens an SSH window. • View Config — Opens the Current Configuration page, where you can view the latest configuration, deploy to running configuration, and/or add comments.
Display results in groups of	You can set the number of items to display per page from the drop-down menu. The default is 25.

Viewing Device Groups

A device group is a method for categorizing your devices in ways that make sense for your organization, for example:

- Geography/physical location
- Business unit/department
- Role in the network architecture
- Activation state

Once created, device groups can be used to direct various features, such as searching, authenticating rules, and updating passwords. Refer to "Adding Device Groups" on page 138 for detailed information on adding device groups.

Initially, the Device Groups page includes one system group: the Inventory group. The Inventory group contains all devices. However, any user-defined groups you create also appear on this page.

To view a list of the device groups, on the menu bar under Devices, click Groups. The Device Groups page opens. Keep in mind that Public device groups are visible to all users. Private device groups are visible only to the owner and NA administrators.

Device Groups Page Fields

Field	Description/Action
New Group link	Opens the New Device Group page, where you can create a new device group. Refer to "Adding Device Groups" on page 138 for information on creating new device groups.
New Parent Group link	Opens the New Parent Group page, where you can add a new parent group. Refer to "Adding Parent Groups" on page 140 for information.
Group Name	Displays the user-defined name of the device group. Parent groups are not indented unless they are also children of other parent groups. Groups that belong to a parent group are indented beneath their parent. Clicking a group name opens the Device Group page, where you can view detailed information about the device group. Refer to "Device Groups Page Fields" on page 190 for information. (**Note**: Group names that are preceded by the cloud icon are included in Partitions. Refer to "Segmenting Devices and Users" on page 150 for information on Partitions.)
Description	Displays a brief description of the group.
Number of devices	Displays the number of devices in the group.
Owner	Displays the user name that created the device group.
Sharing	Displays whether the device group is Public or Private. All users can see Public device groups, while only the owner and the System Administrator can see Private device groups.

Field	Description/Action
Actions	The Actions field for the Inventory group is empty until you select a Group Name. User-defined device groups display the following actions: • View — Displays the devices contained in the selected device group. The devices can either be direct children of this device group if this is a leaf device group, or they could be children of child groups if the device group is a parent device group. Refer to "Device Groups Page Fields" on page 147 for more information on the View option. • Edit — Opens the Edit Group page, where you can edit the information for the device group. • Delete — Enables you to delete the device group. • Diagram — Diagramming enables you to gather topology data from your network devices. Refer to "Diagramming" on page 609 for information. • Make Private/Make Public — Enables you to designate the device group as Public or Private. All users can see Public device groups, while only the owner and the System Administrators can see Private device groups.

Reserving Devices

For organizations with large networks, managing who is working on which devices and at what times is important. The Device Reservation System enables you to reserve a device or a group of devices for a specific period of time. Device Reservation conflict notification prevents you from accidentally working on devices that are already under maintenance and allows a large IT group to schedule and work on the network in a controlled, organized fashion. (Refer to "Workflow" on page 61 for information on configuring the Device Reservation System and the Activity Calendar.)

Keep in mind that devices and/or device groups affected by sub-tasks of a multi-task project are automatically reserved for the duration of the tasks. In addition, when a multi-task project is approved, and one or more scheduled tasks include the following read-write tasks (listed below), a check is done to determine if the read-write task affects a currently reserved device. If it does, a device reservation conflict event is created. A device reservation conflict does not prevent you from running the task against the device or device group, however.

Read-write tasks include:

- Deploy Configuration
- Run Command Script
- Deploy Passwords
- Reboot Device
- Synchronize Startup and Running
- Update Device Software

If a multi-task project reserves a device or group of devices, you are informed when a device configuration change is detected on any of the devices.

For information on setting up multi-task projects, refer to "Scheduling Multi-Task Projects" on page 393.

Activity Calendar

The Activity Calendar enables you to view the activity that is taking place on your network. It provides a list of the tasks and device reservations that have been scheduled for any given day, including:

- All tasks scheduled to run on the day being viewed.
- The start time and date of the task.
- The duration of the task.
- The reserved devices and/or device groups on which the tasks are being run against.
- If the task has an uncleared Device Reservation Conflict event.

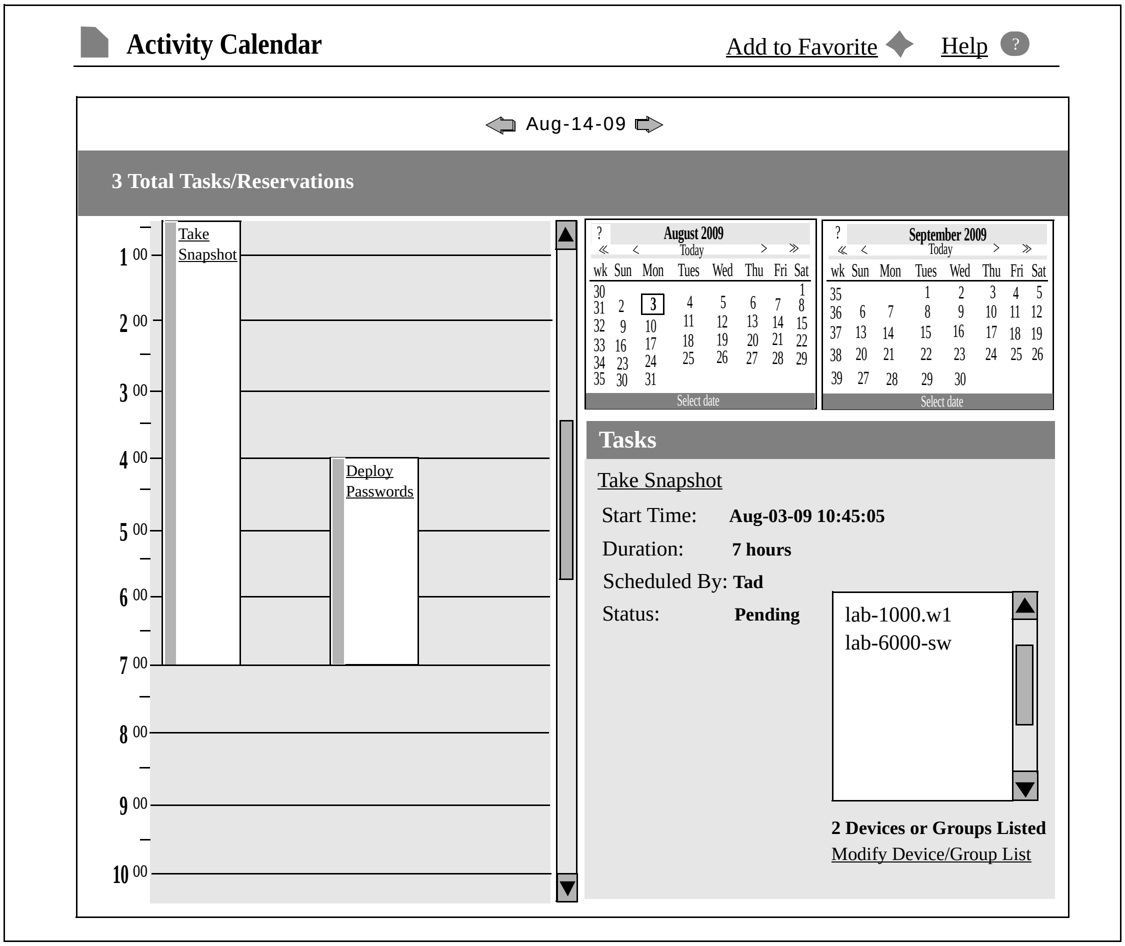
All task blocks start and end on hour or half hour demarcations. Consequently, if a task starts at 22 minutes after the hour, it will be displayed within the row that represents the hour.

The left-hand calendar displays the current month. The right-hand calendar displays the next month. The selected day is highlighted on the appropriate calendar. You can select a specific day by clicking the day listed on the calendar. The page is re-drawn with the appropriate day's events.

Task Details are displayed below the calendars in the right-hand pane. The following task information is provided:

- Start time
- Duration
- The name of the user who scheduled the event
- The status of the event, for example Pending, Running, and Success.

To view the Activity Calendar, on the menu bar under Tasks, click Activity Calendar. The Activity Calendar opens. The following figure shows a sample Activity Calendar display.


Activity Calendar
Add to Favorite
Help
Aug-14-09
3 Total Tasks/Reservations
1 00
2 00
3 00
4 00
5 00
6 00
7 00
8 00
9 00
10 00
Take Snapshot
Deploy Passwords
Select date
Tasks

August 2009

wk	Sun	Mon	Tues	Wed	Thu	Fri	Sat
30							1
31	2	3	4	5	6	7	8
32	9	10	11	12	13	14	15
33	16	17	18	19	20	21	22
34	23	24	25	26	27	28	29
35	30	31					

September 2009

wk	Sun	Mon	Tues	Wed	Thu	Fri	Sat
35			1	2	3	4	5
36	6	7	8	9	10	11	12
37	13	14	15	16	17	18	19
38	20	21	22	23	24	25	26
39	27	28	29	30			

Take Snapshot

Start Time: **Aug-03-09 10:45:05**

Duration: **7 hours**

Scheduled By: **Tad**

Status: **Pending**

lab-1000.w1
lab-6000-sw

2 Devices or Groups Listed

Modify Device/Group List

If you click the link displayed in a cell, the information in the Tasks panel is updated. If a multi-task project has an uncleared device reservation conflict, the cell is highlighted in yellow. For information on configuring a multi-task project, refer to "Scheduling Multi-Task Projects" on page 393.

Viewing Device Details

The Device Details page enables you to perform device-specific tasks. To view the Device Details page:

1. On the menu bar under Devices, click Inventory.
2. On the Inventory page, click a device. The Device Details page opens for that device. (Keep in mind that you can view the Device Details page from most other pages using the Search feature.)

Device Details Page Fields

Field	Description/Action
Hostname	Displays the device’s host name. Clicking the device’s host name opens the Device Details page, where you can view information about this device.
Device IP	Displays the device’s IP address. Clicking the device’s IP address opens the Device Details page, where you can view information about this device.
Last Snapshot Attempt	Displays the date and time the device was last accessed via NA for a snapshot of the device’s configuration.
Last Snapshot Result	Displays the status of the last snapshot of this device’s configuration. If the snapshot failed, there is a link to that Task Result page.
Information Links	When applicable, information on the device is displayed, along with links to more information. For example, if a device is not in compliance with one or more policies, you can click the Policy Events link to open the Policy Activity page. If NA determines that there is a Startup and Running Configurations difference, the following links are displayed: • View Startup — Opens the Device Configuration page. • Compare Startup with Running — Opens the Compare Device Configurations page. • Synchronize — Opens the New Task - Synchronize Startup and Running page.

Field	Description/Action
Watch Device Link	If you click the Watch Device option for the first time, a Watch Group is created, along with a Watch Devices event rule, that includes the device. Any changes to the device will trigger an email notification for the user watching the device. The Watch Devices event rule will send an email notification for a variety of events, such as: • Device Access Failure • Device Booted • Device Configuration Change • Device Deleted • Device Diagnostic Changed • Device Edited • Device Software Change • Software Vulnerability Detected **Note**: You can edit the Watch Devices event rule to change events. All future watched devices will use the same event rule name. Refer to "New Event Notification & Response Rules Page Fields" on page 462. To remove a device from the Watch Group, click Stop Watching Device.
View menu	Opens the View menu. Refer to "View Menu Options" on page 203 for information.
Edit menu	Opens the Edit menu. Refer to "Edit Menu Options" on page 232 for information.
Provision menu	Opens the Provision menu. Refer to "Provision Menu Options" on page 241 for information.
Connect menu	Opens the Connect menu. Refer to "Connect Menu Options" on page 243 for information.
Device Description	Displays the user-defined description of the device, if applicable.
FQDN	Displays FQDN information, if applicable.
Service Type	The Service Type can specify VoIP, BGP, MPLS, and so on. The values help to identify the device's purpose. You can use these values to tag device services so as to easily search for them or view them in a group (static or dynamic). **Note**: You can create custom Service Types via the Admin setting under Device Access. Refer to "Configuration Mgmt Page Fields" on page 38. You can also edit the device to set these values.
Comments	Displays comments, if applicable.
Vendor	Displays the device vendor, such as Nortel or Cisco.
Model	Displays the manufacturer's model number.
Software Version	Displays the version of operating system software running on the device.
Driver Name	Displays the driver assigned to the device.
Device Type	Displays the type of device, such as a router, switch, or firewall.
Serial Number	Displays the manufacturer's serial number for the device.

Field	Description/Action
Asset Tag	Displays your company's asset tag number for the device.
System Memory	Displays the device's system memory.
Location	Typically, the location is obtained in the Configuration file.
Device Origin	Displays the name of the import source if the device was imported into NA and the source was named. If the import source was not named, it states Added to NA on <date>. If the device was added manually, it states Manually added by <user name> on <date>.
Last Successful Snapshot	Displays the date and time the last snapshot succeeded.
Last Configuration Change	Displays the date and time the device's configuration was last changed.
Last Access Attempt	Displays the date and time the device was attempted to be accessed.
Last Access Success	Displays the date and time the device was last successfully accessed.
Change Detection & Polling	Displays either: • Enabled — Indicates that NA periodically polls the device to verify the stored configuration against the device's actual configuration. • Disabled — Indicates the device is not polled periodically or otherwise managed by NA.
Management Status	Displays either: • Active — Indicates that NA records changes to the device's configuration. • Inactive — Indicates that NA does not record changes and that you cannot change the device through NA.
Password Rule	Displays password rule information.
VTP Domain	Displays VLAN Trunking Protocol (VTP) domain name, if applicable.
VTP Operating Mode	Displays the VLAN Trunking Protocol (VTP) operating mode, if applicable.
Ticket Number	Displays the ticket number, if applicable. You can click the Update Ticket button to update the ticket if you have installed one of the NA Connectors.

NA/SA Integration

Implementing changes in an IT environment requires a coordinated effort between network administrators and system administrators. There can be servers running different operating systems and network devices that include firewalls, load balancers, switches, routers, and so on. For example, in some environments, you are required to make changes to network devices that are actually part of an application, such as load balancers and firewalls.

Integrating HP Network Automation (NA) with HP Server Automation (SA) enables you to:

- View Layer 1 connectivity between SA servers and NA network devices. Keep in mind that NA only infers the location of the wiring. NA uses heuristics (as best it can) to determine the physical connections between devices and/or servers. Refer to the *HP Server Automation User's Guide* for information on SA.
- View Layer 2 connectivity between SA servers and NA network devices. NA reduces the number of data link connections between devices and/or servers to make network diagrams more readable. Only connections that can be inferred through transitive connections are reduced. Refer to "Diagramming" on page 609 for information.
- View information on SA servers that are seen by a given NA network device and conversely view which network device can see a given SA server.

To set up NA/SA integration, you must run the NA Topology Data Gathering diagnostic. This diagnostic instructs NA to collect MAC addresses for all switches. MAC addresses are required to discover and add Layer 2 and Layer 1 connections.

In some cases, Layer 1 connectivity (wiring) can be inferred from the Layer 2 connectivity (ARP tables). This enables you to detect configuration mismatches, such as duplex and speed settings.

- Refer to "User Authentication" on page 75 for information on configuring NA/SA integration.
- Refer to "Diagramming" on page 609 for information on creating network diagrams.
- Refer to "Interface Detail Page Fields" on page 208 for information on viewing interface details, including duplex and speed settings.
- Refer to "Servers Page Fields" on page 224 for information on viewing SA servers.

NA/SA Permissions

When integrating NA and SA, the same username and password is used to login to both systems. Keep in mind, however, a user's SA permissions control what SA servers can be viewed by that user in both SA and NA. Similarly, a NA user's permissions control what network devices can be viewed by that user in both NA and SA.

When configuring NA, you can specify a SA username and password. Refer to "User Authentication Page Fields" on page 79 information. The SA user's permissions control what SA servers are discovered by NA when it reads the MAC addresses via the Topology Gathering Diagnostic. Because users can see only the SA servers for which they have permissions, it is recommended that you specify a SA user that can view all SA servers. This ensures that all known SA servers are mapped to appropriate MAC addresses in NA.

For example:

- Server1's MAC address is 0060839488A1.
- SA User A can view Server1.
- SA User B cannot view Server1.
- Switch S7 is connected to Server1.

If NA is configured to use SA User A as the Twist Server username, NA maps 0060839488A1 to Server1 when the Topology Gathering Diagnostic runs. If SA User A logs into NA, he/she can view Server1 on the Servers page (from the Device Details page) for Switch S7. If SA User B logs into NA, he/she cannot view Server1 on the Servers page because he/she does not have permission to view Server1.

Device Hardware Information

In addition to basic hardware details about managed SA servers and NA network devices, NA/SA integration also reports on the following information about network interfaces:

- On the server side, network interfaces identify the ethernet interface, MAC address, devices connected, VLAN name, duplex and speed settings, and so on.
- On the network device side, network interfaces identify the Ethernet port, speed and duplex settings, and connected devices. Auto-negotiate modes are set on a network interface in NA and are then negotiated on a network card in SA. You can create policies that define this configuration, such as a policy that specifies duplex as Full (Auto) and speed as 100 (Auto).

Refer to "Device Interfaces Page Fields" on page 207 for information.

Connecting to NA Through a Firewall

The NA Application Program Interface (API) uses Java Remote Method Invocation (Java RMI) to connect to the NA server. Java RMI can run over various protocols. NA supports Java RMI only over Java Remoting. When integrating SA and NA, SA uses the NA API. As a result, Java RMI and jboss Remoting use the following ports:

- Java Naming and Directory Interface (JNDI) (typically port 1099)
- RMI (typically a dynamic 1098)
- RMI Object (typically port 4446)

To use the NA Java API through a firewall, do the following:

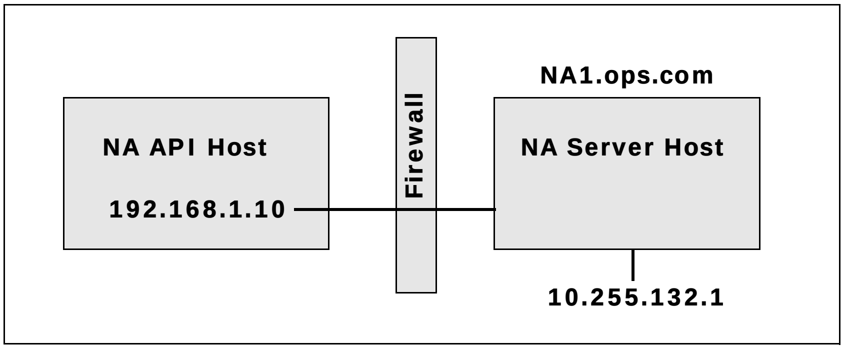
1. Open the following ports through the firewall:
   - Java Naming and Directory Interface (JNDI) (typically port 1099)
   - RMI (typically a dynamic 1098)
   - RMI Object (typically port 4446)

2. Determine next steps.
   - If the NA application server host has the same IP address on both sides of the firewall, configuration is complete.
   - If the NA application server host has a different IP address outside the firewall, continue with step 3.
3. Configure NA to use the RMI server hostname (instead of the IP address) by creating the following file:
   - *Windows*:
     `<NA_HOME>\server\ext\jboss\server\default\conf\jnp.properties`
   - *UNIX*:
     `<NA_HOME>/server/ext/jboss/server/default/conf/jnp.properties`

   This file should include the following line:

   ```
   java.rmi.server.useLocalHostname=true
   ```
4. Save the file and restart the NA server.
5. Ensure that the hostname resolution is correct on the NA server host and on the NA API host (i.e., the SA server host when integrating SA and NA).

   In the following example, NA is running on a host named NA1.ops.com with an IP address of 10.255.132.1. Outside the firewall, to access NA1.ops.com, use 192.168.1.10. The NA Server Host (10.255.132.1) must correctly resolve to NA1.ops.com. On the NA API Host, NA1.ops.com must correctly resolve to 10.255.132.1.



At a high level, the Java RMI/jboss Remoting performs as follows:

1. The client connects to the JNDI port (1099) on host 10.255.132.1.
2. The client queries: Where is bean Connect?
3. The server replies: On port 1098 on host na1.ops.com.
4. The client looks up the IP address for na1.ops.com.
5. The client connects to port 1098 on host 10.255.132.1.
6. If the client requires new Java.class files, the client connects to port 4446 on host 10.255.132.1.

Changing Ports

To change the JNDI port, do the following:

1. Edit the following file to change 1099 to 1199, for example:
    - *Windows*: `<NA_HOME>\server\ext\jboss\server\default\conf\bindingservice.beans\META-INF\bindings-jboss-beans.xml`
    - *UNIX*: `<NA_HOME>/server/ext/jboss/server/default/conf/bindingservice.beans/META-INF/bindings-jboss-beans.xml`
2. Save the file and restart the NA server. (**Note**: If you change the JNDI port, the code calling the NA API will also need to be changed. Instead of connecting to NA1.ops.com:1099, for example, the NA API will have to connect to NA1.ops.com:1199 (or whatever port is configured).

To change the RMI port, do the following:

1. Edit the following file to change 1098 to 1198, for example:
    - *Windows*: `<NA_HOME>\server\ext\jboss\server\default\conf\bindingservice.beans\META-INF\bindings-jboss-beans.xml`
    - *UNIX*: `<NA_HOME>/server/ext/jboss/server/default/conf/bindingservice.beans/META-INF/bindings-jboss-beans.xml`
2. Save the file and restart the NA server. (**Note**: Changes to the RMI Port are transparent to the client. No client changes are required.)

To change the RMI Object port, do the following:

1. Edit the following file to change 4446 to 4447, for example:
    - *Windows*: `<NA_HOME>\server\ext\jboss\server\default\conf\bindingservice.beans\META-INF\bindings-jboss-beans.xml`
    - *UNIX*: `<NA_HOME>/server/ext/jboss/server/default/conf/bindingservice.beans/META-INF/bindings-jboss-beans.xml`
2. Save the file and restart the NA server. (**Note**: Changes to the RMI Object Port are transparent to the client. No client changes are required.)

Incorrect Port Counts

If port counts are incorrect, do the following to configure which port types are counted:

1. Stop NA.
2. Update the *$NA/adjustable_options.rcx* file and add the following entries anywhere between the `<options>` and `</options>` tags:

```
<array name="PortCount/PortTypes">
<value>Ethernet</value>
<value>FastEthernet</value>
<value>GigEthernet</value>
<value>FDDI</value>
<value>Lex</value>
<value>TokenRing</value>
<value>VGAnyLan</value>
<value>Pos</value>
<value>Serial</value>
<value>HSSI</value>
<value>ATM</value>
<value>Dialer</value>
<value>BRI</value>
<value>DSL</value>
<value>TenGigabitEthernet</value>
<value>GigEthernetTrunk</value>
</array>
```

   Note: Edit the above list as appropriate for the interface/port types that you want counted.

3. Replace `$NA` with the location where NA has been installed, typically */opt/na*.
4. Update the *$NA/adjustable_options.rcx* file and add the following entry anywhere between the `<options>` and `</options>` tags:

```
<option name="snapshot/force_update_model_data">true</option>
```

   Note: This option causes NA to recompute the port counts (and other device data) on every checkpoint snapshot even if there is no configuration change.

5. Restart NA.
6. Run a Snapshot task against Inventory to update the port counts.
7. Check the “Make snapshot a checkpoint” option on the New Task page. This will recompute the port counts for existing devices.

   Note: Note: After running the Snapshot task, you might want to remove `<option name="snapshot/force_update_model_data">true</option>` from the *$NA/adjustable_options.rcx* file to improve performance.

View Menu Options

Menu Option	Description/Action
Device Detail	You can select the following options: • Device Home — Opens the Device Details page for that device. • ACLs — Opens the Device ACLs page, where you can view a list of all ACLs associated with this device. Refer to “Viewing ACLs” on page 685 for information. • Interfaces — Opens the Device Interfaces page, where you can view the device’s interfaces and a list of upstream and downstream devices connected via each interface. When a connected device is actively managed, there is a link to that device. This enables you to traverse the Layer 3 topology when troubleshooting without having to look up your network diagrams. (**Note**: The Device Interfaces page is updated when you run the Interfaces diagnostic. By default, this diagnostic runs when NA detects a configuration change.) Refer to “Device Interfaces Page Fields” on page 207 for information. • IP Addresses — Opens the Device IP Addresses page, where you can view all IP addresses that are associated with the device. This includes the IP addresses of interfaces on the device, as well as IP addresses on the network that are visible to the device. Refer to “Device IP Addresses Page Fields” on page 213 for information. • MAC Addresses — Opens the Device MAC Addresses page, where you can view a list of all MAC addresses known to NA that are associated with the device. Refer to “Device MAC Addresses Page Fields” on page 214 for information. • VLANs — Opens the Device VLANs page, where you can view VLAN information as it is configured on the device. Refer to “Device VLANs Page Fields” on page 217 for information. • VTP Information — Opens the VTP Detail page, where you can view VTP information for a VLAN. Refer to “VTP Detail Page Fields” on page 220 for information. • Modules — Opens the Device Blade/Modules page, where you can view a list of the modules (blades, cards) installed on the device. By default, the module data is updated weekly by the Module Status diagnostic. Refer to “Device Blades/Modules Page Fields” on page 222 for information. • Policies — Open the Device Policies page, where you can Verify that the correct policy was applied to the device, view if the policy passed or failed, view policies that are applied to the device when the device is added to NA, and view the exceptions that are in place for a policy applied to the device. Refer to “Device Policies Page Fields” on page 223 for information. • Servers — Opens the Servers page, where you can view a list of HP Server Automation (SA) servers that are connected to the device. Refer to “Servers Page Fields” on page 224 for information. • Software Upgrade Recommendation — Opens the Software Upgrade Recommendation page, where you can view all device software image recommendations, minus the ones you removed by the filters designated on the My Preference page. Refer to “Device Software Image Recommendation Page Fields” on page 225 for information.
SingleView	Opens the SingleView page, where you can track events that indicate changes to either a single device or all of your devices on one page. Refer to “Consolidated View of Events (SingleView)” on page 552 for information.
Current Configuration	Opens the Current Configuration page, where you can deploy the configuration to the running configuration on the device. Refer to “Device Configurations Page Fields” on page 175 for information.

Menu Option	Description/Action
Configuration Changes	Opens the Device Configurations page, where you can view two device configurations side-by-side. Refer to "Comparing Device Configurations" on page 181 for information.
Diagnostics	Select an option from the Diagnostics list. Each option shows a historical list of diagnostics specific to the device. The most frequently employed diagnostics include: • All — Displays all of the diagnostics on one page. • Basic IP — Displays the basic IP information, such as the default gateway, DNS servers, Domain list, and the IP addresses assigned to installed interfaces. • Memory Troubleshooting — This diagnostic is a sample custom diagnostic that is implemented for some devices. It is included as a standard diagnostic after a device configuration change. • Device Information — Displays basic device information, such as software and hardware versions, the model and host name of the device, and interface descriptions. Although this information appears with the default diagnostics, it is updated only when NA runs a snapshot task on the device. • NA Detect Device Boot — Displays information on when the device was last booted. • NA Device File System — Records what files (generally software image files) are currently on the device's flash cards or hard drive. This data is used by the Deploy Software task. • NA Duplex Data Gathering — Gathers Layer 2 connectivity data, such as duplex settings and the current port state, for Interface reports. Note that not all devices support this diagnostic. In addition, it does not have any viewable diagnostic output. • NA Flash Storage Space — This diagnostic is special-purpose diagnostic used only against Nortel BayRS devices to trigger a low-flash space event, which then causes a compression script to run. • NA Interfaces — Displays the interfaces information for the device, such as state, IP address, errors, I/O rate, and VLAN information. • NA Module Status — Displays the module diagnostics for this device. • NA OSPF Neighbors — Displays a list of the OSPF neighbor tables stored in the NA database. • NA Routing Table — Displays all the routing tables for this device stored in the NA database. If BGP is running, it shows the Routing Table summary information, when available. • NA Topology Data Gathering — This diagnostic is used to populate the tables used for diagramming and topology reports. It does not have any viewable diagnostic output. • NA VLAN Data Gathering — This diagnostic is used to gather the latest VLAN information. The information on the New Device VLAN and Edit Device VLAN pages is based on the last time VLAN data was gathered from the device. To ensure that you have the latest VLAN data, run the VLAN Data Gathering diagnostic to update NA with the latest VLAN data. (**Note**: This diagnostic does not result in storing any diagnostic text in the database. The diagnostic only updates certain tables in the database. As a result, the diagnostic is not viewable.) • NA Port Scan — This diagnostic uses Nmap to scan a device's ports and return details on which ports are open and what services they provide.
Device Tasks	Opens the Device Tasks page, where you can view a list of all tasks associated with this device. You can also view details about the task or rerun the task from this page. Refer to "Device Tasks Page Fields" on page 227 for information on the Device Tasks page.

Menu Option	Description/Action
Device Events	Opens the Device Events page, where you can view recent system events for the device, including their success/failure status, and access detailed information about the event by clicking the link in the Summary field. Refer to "Device Events Page Fields" on page 206 for information on the Device Events page fields.
Device Relationships	Opens the Device Relationships page. Device relationships enable you to create a relationship between devices and then view the relationships. Refer to "Device Relationships Page Fields" on page 228 for information on the Device Relationships.
Software Audit Trail	Opens the Device Software History page, where you can view what software is loaded on the device. Refer to "Device Software History Page Fields" on page 230 for information on the Device Loaded Software page fields.
Telnet/SSH Sessions	Opens the Device Session page, where you can view a list of the Telnet and SSH sessions associated with the device. Sessions can include only the commands or the keystroke logging for the entire session. Refer to "Device Sessions Page Fields" on page 231 for information on the Device Session page fields.

Keep in mind that most of the NA diagnostics are standard diagnostics that are shipped with the product and cannot be edited, with the exception of the following sample diagnostics:

- Memory Troubleshooting
- Hardware Information

Device Events Page Fields

The Device Events page enables you to view recent system events for the device, including their success/failure status, and access detailed information about the event.

Field	Description/Action
Check Boxes	You can use the left-side check boxes to delete selected events. Once you have selected events, click the Actions drop-down menu and click Delete. The adjacent Select drop-down menu enables you to select or deselect all of the events.
Event Date	Displays the date and time the event occurred.
Summary	Displays a brief summary of the event. If you click the Summary link, the Event Detail page opens, where you can view detailed information about the event.
Added By	Displays the person or process that initiated the event.

Device Interfaces Page Fields

The Device Interfaces page enables you to view the device's interfaces and a list of upstream and downstream devices connected via each interface. Keep in mind that although a Port is a Layer 2 term and Interface is a Layer 3 term, NA does not make that distinction.

To view the Device Interfaces page, on the View menu for a device, select Device Details and click Interfaces. The Device Interfaces page opens.

Field	Description/Action
Port Name	Displays the name of the port, such as Ethernet0 or Serial1.
Port Type	Displays the name of the port type, such FastEthernet.
Port Status	Displays if the interface is Configured Up or Administratively Down. (**Note**: This does not reflect the protocol state of the interface, only the configured state.)
Running Port State	Specifies the Layer 2 connectivity of the port (up or down). This information is gleaned from the NA Duplex Data Gathering diagnostic. Refer to "Run Diagnostics Task Page Fields" on page 312 for information.
Port IP	Displays the primary IP address for the interface. NA parses the IP address from the device configuration. Refer to "Device Configurations Page Fields" on page 175 for information.
Description	Displays a brief description of the interface. NA parses the description from the device configuration.
Negotiated Duplex	Displays the negotiated duplex, either full or half. This information is gathered by the Gather Topology Data Diagnostic. Refer to"Run Diagnostics Task Page Fields" on page 312 for information.
Actions	You can select the following actions for each interface: • Edit Interface — Opens the Edit Interface Detail page, where you can edit the details about this interface and any custom data fields. Refer to "Edit Interface Detail Page Fields" on page 210. • View Interface — Opens the Interface Detail page, where you can view details about this interface and custom data, view alternate IP addresses, the connected servers, and view or edit comments. Refer to "Interface Detail Page Fields" on page 208. For detailed information on SA server management, refer to the *HP Server Automation User's Guide*. • Interfaces in Subnet — Opens the Interfaces in Subnet page, where you can view all the interfaces in the same subnet as this interface. This enables you to traverse the devices linked within the subnet, as long as the devices are actively managed. Refer to "Interfaces in Subnet Page Fields" on page 212.

Interface Detail Page Fields

The Interface Detail page enables you to view details for a specific interface. Keep in mind that although a Port is a Layer 2 term and Interface is a Layer 3 term, NA does not make that distinction.

Field	Description/Action
Device	Displays the name and IP address of the device.
Name	Displays the interface name, for example: Ethernet0/1
Type	Displays the type of interface, for example: Ethernet
Status	Displays the status of the interface, for example: Configured Up
Connected to	Displays the servers to which the interface is connected.
Primary IP	Displays the interface's Primary IP address. If you click the Interfaces in Subnet link, the Device Interfaces page opens, where you can view all the interfaces in the same subnet as this interface. This enables you to traverse the devices linked within the subnet, as long as the devices are actively managed. "Device Interfaces Page Fields" on page 207 for information.
Description	Displays a description of the interface.
MAC Address	Displays the MAC address of the interface, for example: 00-50-10-F6-41
Member VLANs	Displays the VLANs to which this device belongs. If you click the VLAN name link, the VLAN Detail page opens for the VLAN. Refer to "VLAN Detail Page Fields" on page 219 for information. For detailed information on VLANs, refer to "Virtual Local Area Networks (VLANs)" on page 215. **Note**: If a trunk port does not have a native VLAN (untagged VLAN), "No Native VLAN" is displayed at the bottom of the Member VLANs list.
Duplex	Network interfaces identify the Ethernet port, speed, duplex settings, devices connected, and VLAN name. Auto-negotiate modes are set on a network interface in NA and are then negotiated on a network card in SA. A duplex mismatch is a configuration mismatch between the speed and duplex of a managed server and a connected network device.
Speed	Network interfaces identify the Ethernet port, speed, and duplex settings, devices connected, and VLAN name. Auto-negotiate modes are set on a network interface in NA and are then negotiated on a network card in SA. A speed mismatch is a configuration mismatch between the speed and duplex of a managed server and a connected network device.
Configuration	Displays the current configuration of the interface. If you click the View Configuration link, the Current Configuration page opens. Configlet parsing enables the parser to extract the lines in the configuration relevant to the interface.

Field	Description/Action
VRF	Displays the section of the device configuration defining the Virtual Routing and Forwarding (VRF) that is associated with the interface. VRF enables multiple instances of a routing table to co-exist within the same router. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other. **Note**: This field is displayed only if the interface has an associated VRF and the device driver supports VRF parsing.
QoS	Displays Quality of Service (QoS) information. NA parsers the interface configuration for QoS configuration statements and displays the corresponding global configuration information. In other words, parts of the configuration that are related to, but not included in the interface configuration, are shown. This includes route-maps, policy-maps, class-maps, and ACLs. This information provides a broader view of the device configuration and why the network is performing as it is (packet loss, long delays for certain packet types, and so on).
ACLs	Displays the ACLs that are known to exist on the interface.
Last Modified	Displays when the interface was last modified.
Comments	Displays any comments about the interface.
Edit Detail link	Opens the Edit Interface Detail page. "Edit Interface Detail Page Fields" on page 210.

Edit Interface Detail Page Fields

The Edit Interface Detail page enables you edit the details for an interface and any custom data fields.

To navigate to the Edit Interface Detail page:

1. From the Device Details page, select the View menu.
2. From the View menu, select Device Detail and click Interfaces. The Device Interfaces page opens.
3. In the Actions field, click the Edit Interface link for the port you want to edit. The Edit Interface Detail page opens.

Note: The Edit Interface Detail page includes a section to configure trunk ports. The VLAN Trunk checkbox enables you to set up a trunk port. The section is a collapsible set of fields that are displayed when checked, including “Native VLAN ID” and “Member VLANs”, as described in the table.

Field	Description/Action
Device	Displays the name and IP address of the device.
Name	Displays the interface name, for example: Ethernet0/1
Type	Displays the type of interface, for example: Ethernet
Status	Displays the status of the interface, for example: Configured Up
Connected to	Displays the servers to which the interface is connected.
Primary IP	Displays the interface’s Primary IP address. If you click the Interfaces in Subnet link, the Device Interfaces page opens, where you can view all the interfaces in the same subnet as this interface. This enables you to traverse the devices linked within the subnet, as long as the devices are actively managed.
Description	Displays a description of the interface.
MAC Address	Displays the MAC address of the interface, for example: 00-50-10-F6-41
Member VLANs	Displays the VLANs to which this device belongs. For detailed information on VLANs, refer to “Virtual Local Area Networks (VLANs)” on page 215.
Duplex	Network interfaces identify the Ethernet port, speed, duplex settings, devices connected, and VLAN name. Auto-negotiate modes are set on a network interface in NA and are then negotiated on a network card in SA. A duplex mismatch is a configuration mismatch between the speed and duplex of a managed server and a connected network device.
Speed	Network interfaces identify the Ethernet port, speed, and duplex settings, devices connected, and VLAN name. Auto-negotiate modes are set on a network interface in NA and are then negotiated on a network card in SA. A speed mismatch is a configuration mismatch between the speed and duplex of a managed server and a connected network device.

Field	Description/Action
VLAN Trunk	Certain ports can be configured as trunk port, physical ports, and port channels (aggregated links). Loop-back ports and ports for VLAN interfaces cannot be configured as trunk. Unchecking a VLAN Trunk sets a port as non-trunk. As a result, the port is assigned to the VLAN indicated in Native VLAN ID field. Any modification of the VLAN trunk port settings results in creating a new VLAN task to apply the changes on the device. Refer to "VLAN Task Page Fields" on page 365 for information. **Note**: The VLAN Trunk field is not displayed on the Edit Interface Detail page if the device driver does not support the enhanced VLAN functionality.
Native VLAN ID	The Native VLAN ID is a VLAN whose packets are not tagged on the trunk port. In addition, any untagged packets received on the port are considered those of the Native VLAN. Note that Native VLAN is a Cisco term. For example, the ProCurve does not use the Native VLAN terminology. The ProCurve uses the untagged VLAN membership terminology. A trunk port can have only one untagged VLAN membership.
Member VLANs	The VLAN trunk port transports the traffic of the selected VLANs. Any VLANs that are not selected will be pruned.
Specify VLAN ID	For Cisco devices, any VLAN ID or VLAN ID range can be specified for a trunk port. Trunk ports on Cisco devices can be members of VLANs that are not defined on the device. (Note that this field is not displayed for non-Cisco devices.)
Comments	Displays any comments about the interface.

Interfaces in Subnet Page Fields

The Interfaces in Subnet page enables you to view the interfaces in a subnet, along with the negotiated duplex and negotiated speed settings. The Layer 3 interfaces are compared to other interfaces in the subnet. If there is a mismatch, the mismatched ports display their value in bold, red text.

Field	Description/Action
Host Name	Displays the name host or IP address on which the interface resides.
Port Name	Displays the name of the port, such as Ethernet0 or Serial1.
Port Status	Displays if the interface is Configured Up or Administratively Down. (**Note**: This does not reflect the protocol state of the interface, only the configured state.)
Port IP	Displays the primary IP address for the interface. NA parses the IP address from the device configuration.
Description	Displays a brief description of the interface. NA parses the description from the device configuration.
Negotiated Duplex	Displays the negotiated duplex, either full or half. This information can be used to determine if traffic through a switch is impacted by another switch operating at either full duplex, 100M, or half duplex, 10M. For example, you might have switch on the network that is forced to queue packets due to a delay on part of the path.
Negotiated Speed	Displays the negotiated speed, such as 100M.
Actions	You can select the following actions for each interface: • Edit Interface — Opens the Edit Interface page, where you can edit the details about this interface and any custom data fields. • View Interface — Opens the Interface Detail page, where you can view details about this interface and custom data, view alternate IP addresses, the connected servers, and view or edit comments. Refer to "Interface Detail Page Fields" on page 208. For detailed information on SA server management, refer to the *HP Server Automation User's Guide*.

Device IP Addresses Page Fields

The Device IP Addresses page enables you to view all IP addresses that are associated with the device. This includes the IP addresses of interfaces on the device, as well as IP addresses on the network that are visible to the device.

Field	Description/Action
Port Name	Displays the port name associated with the device's IP address.
Address	Displays the IP address.
Address Type	Displays the type of IP address, for example: "Address of Port" or "Seen from Port".
VLAN	Provides a link to the VLAN, if any, containing this IP address if the type is "Address of Port".
Description	Provides a description of the IP address.
Remote Location	Provides links to the remote location if the type is "Seen from Port". The remote location is a device and port known to NA (or if NA/SA integration is enabled, a server and interface known to SA).
First Seen	Displays the date and time the IP address was first identified.
Last Seen	"Current" is displayed if the IP address was seen the last time NA gathered topology data. If not current, this is the date and time when NA last saw the IP address on the network. Keep in mind that the IP address is possibly no longer on the network, for example an IP address of a laptop or other transient device. In addition, the routing traffic could change such that the IP address is no longer in the main flow.
Associated MAC	Opens the Device MAC Addresses page, where you can view a list of all MAC addresses known to NA that are associated with the device.
Actions	You can select the following actions for each device: • View Details — Opens the IP Address Details page, where you can view details on the following information: Device, Device Port, IP address, MAC Address, Type, First Seen, and Last Updated. • View MAC - Opens the MAC Address Details page that is cross-referenced with this IP address. Cross-referencing means that when NA gathers data, the IP address and MAC address were indicated as coming from the same source. This is only available on "seen from port" records.

Device MAC Addresses Page Fields

The Device MAC Addresses page enables you to view a list of all MAC addresses that are associated with the device.

Field	Description/Action
Port Name	Displays the port name associated with the device's IP address.
Address	Displays the device's MAC address.
Address type	Displays the type of the MAC address, for example: "Address of Port" or "Seen from Port".
VLAN	Provides links to the VLAN, if any, containing this MAC address if the type is "Address of Port".
Description	Displays the description of the MAC address.
Remote Location	Provides links to the remote location if the type is "Seen from Port". The remote location is a device and port known to NA. This could alternately be a server and interface known to HP Server Automation (SA). Refer to "NA/SA Integration" on page 198 for information on NA/SA integration.
First Seen	Displays the date and time the MAC address was first identified.
Last Seen	"Current" is displayed if the MAC address was seen the last time NA gathered topology data. If not current, this is the date and time when NA last saw the MAC address on the network. Keep in mind that the MAC address is possibly no longer on the network, for example a MAC address on a laptop or other transient device. In addition, the routing traffic could change such that the MAC address is no longer in the main flow.
Associated IP	Opens the Device IP Addresses page, where you can view a list of all IP addresses known to NA that are associated with the device.
Actions	You can select the following actions for each device: • View Details — Opens the MAC Address Details page, where you can view details on the following information: Device, Device Port, MAC address, Type, Configuration snippet, First Seen, and Last Updated. • View IP - Opens the IP Address Details page, where you can view details on the Device, Device Port, IP Address, MAC Address, Type, First Seen and Last Updated. • that is cross-referenced with this IP address. Cross-referencing means that when NA gathers data, the IP address and MAC address were indicated as coming from the same source. This is only available on "Seen from Port" records.

Virtual Local Area Networks (VLANs)

VLANs (Virtual Local Area Networks) are conglomerations of ports that act as a single broadcast domain. VLANs operate at Layer 2 (the Data Link layer) which modifies the Ethernet frame with the VLAN tag to provide broadcast domain segmentation and group device across network switches. NA gathers information about what VLANs are defined on a managed device and the VLAN to which each port is assigned.

In general, a VLAN segments broadcast domains so as to group end-stations together even if they are not located in the same network switch. VLANs enable network switches to be virtualized, meaning that a network switch can serve more than one Layer 2 network and a LAN spanning multiple network switches.

Because VLANs provide segmentation services, they address security, scalability, and network management issues in Layer 2 without using network routers. Different broadcast domains provide security within organizations because they isolate the traffic of one domain from the others.

For example in an enterprise environment, the Finance Department, Human Resources Department, and Sales Department can have their own broadcast domain so that their traffic cannot be seen by the other departments. In addition, the Finance Department could have employees in different facilities. As a result, a VLAN can group them together as if they were in one physical location connected to the same network switch, increasing the scalability of the network.

VLANs also provide virtualization for network switches by enabling a network switch to be segmented into multiple broadcast domains and enabling multiple network switches to be part of a broadcast domain. Therefore, instead of having a separate network switch for each department within an organization, a network switch can be divided into virtual network switches with VLANs to serve multiple departments.

NA enables you to view and provision VLANs on network switches. With NA, you can:

- View a complete list of a device’s VLANs
- View specific VLAN details
- View a list of ports assigned to a VLAN
- View trunk ports
- View a list of VLANs on a trunk port
- View the native VLAN of a trunk port (the VLAN whose traffic on the trunk port is not tagged)
- View VTP settings of a network switch
- Create a new VLAN on a network switch
- Change a port assigned to a VLAN (add/prune ports)
- Change a VLAN’s name
- Delete a VLAN
- Configure a port as a trunk port (multiple VLAN with tagging)
- Change trunk port VLANs (VLAN membership)

- Change trunk port native VLAN
- Configure a trunk port as a non-trunk

Device VLANs Page Fields

The Device VLANs page displays a list of all VLANs on the device. For detailed information on VLANs, refer to “Virtual Local Area Networks (VLANs)” on page 215.

To navigate to the Device VLANs page:

1. From the Inventory page, select the device for which you want VLAN details. Note that you can also use the Search options on any page to locate devices. The Device Details page opens.
2. On the Device Details page, select the View menu.
3. From the View menu, select the Device Details option and click the VLANs option. The Device VLANs page opens.

Note: If a device driver does not support the enhanced VLAN features, provisioning actions are not displayed.

Field	Description/Action
New VLAN link	Opens the New Device VLAN page, where you can create a new VLAN. Refer to “Creating and Editing VLANs” on page 218 for information.
VLAN	Displays the VLAN name.
VLAN Type	Displays the VLAN type. This field is vendor specific.
VLAN ID	Displays the VLAN’s ID.
VLAN Status	Displays the VLAN’s status, such as active or suspended.
Last Modified	Displays the date and time NA last read the VLAN from the device. (Note that NA might have read the VLAN from the device since this date and time, but there is no change.)
Description	Displays information about the VLAN pulled from the device.
Actions	You can select the following actions for each VLAN: • View — Opens the VLAN Detail page, where you can view VLAN details. The VLAN Ports information is linked to the Device Interface page. Refer to “VLAN Detail Page Fields” on page 219 for information. Keep in mind that trunk ports are displayed if they are members of the VLAN. • Edit — Opens the Edit VLAN Detail page, where you can view VLAN details and edit the VLAN name, description, and port membership. Refer to “Creating and Editing VLANs” on page 218 for information. • Delete — Opens a dialog box, where you can confirm that you want to delete the VLAN.

Creating and Editing VLANs

The New Device VLAN page enables you to enter a VLAN name and check the ports to be assigned to the new VLAN. The Edit Device VLAN pages enable you to modify the VLAN name and port membership information. For detailed information on VLANs, refer to "Virtual Local Area Networks (VLANs)" on page 215.

Note: The information on the New Device VLAN and Edit Device VLAN pages is based on the last time VLAN data was gathered from the device. Any modifications on the device after the last time VLAN data was gathered is not reflected on these pages. To ensure that you have the latest VLAN data, run the VLAN Data Gathering diagnostic to update NA with the latest VLAN data. Refer to "Run Diagnostics Task Page Fields" on page 312 for information.

Field	Description/Action
Device	Displays the device's host name and/or IP address. If you click the device link, the Device Details page opens. Refer to "Viewing Device Details" on page 195.
VLAN Name	Enter a new VLAN name or edit the existing VLAN name.
VLAN ID	Enter the VLAN ID. Note that the VLAN ID field is text only for the Edit VLAN operation, unlike the New VLAN operation in which the VLAN ID is an input field.
VLAN Type	Displays the VLAN type. This field is vendor specific. This information is automatically populated from data gathered from the device.
VLAN Status	Displays the VLAN's status, such as active or suspended. This information is automatically populated from data gathered from the device.
VLAN MTU	Displays the VLAN Maximum Transmission Unit (packet size) that the VLAN can use. This field is vendor specific. This information is automatically populated from data gathered from the device.
VLAN Ports	Displays a list of VLAN ports. Port names are links to the Interface Detail page for that port. Refer to "Interface Detail Page Fields" on page 208 for information. Ports that are currently assigned to the VLAN are checked. Available ports that are currently not assigned but can be assigned, are not checked. Their Native VLAN name is specified between right parentheses. If the port is a Trunk port, it is stated as such. In addition, if the port is a PortChannel, its Aggregated Ports are displayed in a comma separated list. Ports that are currently assigned to the VLAN can be pruned (removed) from the VLAN by unchecking their checkboxes. Similarly, ports that are not currently assigned to the VLAN can be assigned by checking their checkboxes.
VLAN Description	Displays a description of the VLAN.

Be sure to click the Save button when you are finished. If you have made any modification, the VLAN Task page opens. Refer to "VLAN Task Page Fields" on page 365 for information.

VLAN Detail Page Fields

When you click the View option in the Actions field on the Device VLANs page, the VLAN Detail page opens.

Field	Description/Action
Device	Displays the device's host name and/or IP address. If you click the device link, the Device Details page opens. Refer to "Viewing Device Details" on page 195 for information.
VLAN Name	Displays the VLAN name.
VLAN ID	Displays the VLAN's ID.
VLAN Type	Displays the VLAN type. This field is vendor specific.
VLAN Status	Displays the VLAN's status, such as active or suspended.
VLAN MTU	Displays the VLAN Maximum Transmission Unit (packet size) that the VLAN can use. This field is vendor specific.
VLAN Ports	Displays a list of VLAN ports. If you click a port link, the Interface Details page opens for that port. If a trunk port does not have a native VLAN (untagged VLAN), "No Native VLAN" is displayed at the bottom of the Member VLANs list. Refer to "Interface Detail Page Fields" on page 208. Trunk ports have all VLANs listed on the Device Interface pages. Refer to "Device Interfaces Page Fields" on page 207 for information.
VLAN Description	Displays information about the VLAN pulled from the device.
Last Modified Date	Displays the date and time NA last read the VLAN from the device. (Note that NA might have read the VLAN from the device since this date and time, but there is no change.)
Edit Detail link	Opens the Edit VLAN Details page. Refer to "Creating and Editing VLANs" on page 218 for information.

VTP Detail Page Fields

The VLAN Trunking Protocol (VTP) is a Cisco proprietary protocol to manage VLANs among Cisco switches. VTP defines a management domain called VTP domain. One or more switches in a VTP domain are configured as a server to distribute VLAN configuration so that others do not need to be manually configured. There are three levels of participation (operating modes):

- Server
- Client
- Transparent

Switches configured as a server in a VTP domain advertise any VLAN configuration changes to other switches in the domain. VTP packets are sent to the switches connected to the server. The switches that are in Client mode respond to VTP packets and modify their own VLAN configuration accordingly, and then relay the VTP packets to other switches in the domain. Switches in Transparent mode do not change their VLAN configurations, but rather relay the VTP packets to other switches.

NA displays device VTP information if the device is a Cisco switch and the device participates in a VTP domain. For detailed information on VLANs, refer to "Virtual Local Area Networks (VLANs)" on page 215.

Note: NA does not provision VTP settings. NA's VTP support is read-only, meaning that NA only gathers VTP information from devices for display.

To navigate to the VTP Details page:

1. From the Inventory page, select the device for which you want VTP details. Note that you can also use the Search options on any page to locate devices. The Device Details page opens.
2. On the Device Details page, Select the View menu and click the VTP Information option. The VTP Details page opens.

Field	Description/Action
Device	Displays the device's host name and/or IP address. If you click the device link, the Device Details page opens. Refer to "Viewing Device Details" on page 195 for information.
VTP Version	Displays the VTP version.
Configuration Version	Displays the configuration version number.
Domain Name	Displays the VTP Domain Name. The name is a link to the VTP Domain's page, where you can view a list of devices that belong to that domain. Refer to "VTP Domain Page" on page 222 for information. (**Note**: VTP Domain Names containing single quotation marks (') cause NA to return a SQL error.)
Maximum VLANs Supported Locally	Displays the maximum number of locally supported VLANs.
Number of Existing VLANs	Displays the number of existing VLANs.

Field	Description/Action
VTP Operating Mode	Displays the VTP’s operating mode, including Server, Client, Transparent, or Off.
VTP Pruning Mode	If enabled, VTP pruning enables you to remove unnecessary traffic caused by unknown unicasts and broadcasts.
VTP V2 Mode	If enabled, VTP 2 mode can be used for Token Ring VLANs.
VTP Traps Generation	If enabled, VTP traps can be generated for troubleshooting.
MD5 Digest	If enabled, MD5 Digest can be used for troubleshooting. MD5 Digest displays a 16-byte word (MD5 value) constructed from a combination of the VTP Password (if configured) and the VTP Domain Name.
VTPs in This Domain	Displays the devices in the domain. The devices' Hostname and/or IP Address is a link to the Device Details page. The device’s details page includes VTP domain name and operating mode information if a device has VTP configuration. Refer to “Device Details Page Fields” on page 195 for information.
Last Modified By	Displays who last modified the VTP.
Last Modified Date	Displays the date the VTP was last modified.

VTP Domains Page Fields

The VLAN Trunking Protocol (VTP) Domains page lists the VTP domains in the network of one or more devices that NA manages. For detailed information on VLANs, refer to “Virtual Local Area Networks (VLANs)” on page 215.

To navigate to the VTP Domains page, from the Devices menu, select Device Tools and click the VTP Domains option. The VTP Domains page opens.

Field	Description/Action
Domain Name	Displays the domain name.
VTP Version	Displays the VTP version.
Number of Devices	Displays the number of devices NA is aware of in the domain.
Actions	If you click the View link, the VTP Domain page opens. Refer to “VTP Domain Page” on page 222 for information.

VTP Domain Page

The VTP Domain page displays the devices in a specific domain. For detailed information on VLANs, refer to "Virtual Local Area Networks (VLANs)" on page 215.

To navigate to the VTP Domain (domain_name) page, on the VTP Domains page, click the View option in the Actions field for the domain for which you want to view device details. The VTP Domain page opens.

Field	Description/Action
Host Name	Displays the host name of the device. If you click the Host Name link, the Device Details page opens. Refer to "Viewing Device Details" on page 195 for information.
Device IP	Displays the Device's IP address. If you click the Device IP link, the Device Details page opens. Refer to "Viewing Device Details" on page 195 for information.
MD5 Digest	If enabled, MD5 Digest can be used for troubleshooting.
Operating Mode	Displays the VTP operating mode, for example Server, Client, Transparent, or Off.
Partition	Displays the Partition to which the device belongs. (**Note**: This field is only displayed if you have configured one or more Partitions.)
Actions	You can select the following actions: • View VTP — Opens the VTP Detail page. Refer to "VTP Detail Page Fields" on page 220 for information. • View VLANs — Opens the Device VLANs page. Refer to "Device VLANs Page Fields" on page 217 for information.

Device Blades/Modules Page Fields

The Device Blade/Modules page lists the modules (blades, cards) installed on the device. By default, the module data is updated weekly by the Module Status Diagnostic task.

Field	Description/Action
Module Slot	Displays the slot on the device in which the module is installed.
Module Description	Displays a brief description of the module. NA parses the description from the device configuration.
Module Model	Displays the model identifier.
Module Serial	Displays the module's serial number.
Actions	You can select the following actions for each module: • Edit Module — Opens the Edit Blade/Module Detail page, where you can view the module inventory details and edit the custom data fields. • View Module — Opens the Blade/Module Detail page, where you can view the module inventory details and edit the comments.

Device Policies Page Fields

The Device Policies page enables you to:

- Verify that the correct policy was applied to the device.
- View if the policy passed or failed.
- View policies that are applied to the device when the device is added to NA.
- View the exceptions that are in place for a policy applied to the device.

For information on creating polices, refer to "How the NA Policy Manager Works" on page 415. For information on how to view applied polices, refer to "Viewing Applied Policies" on page 431.

Field	Description/Action
Policy Name	Displays the policy name.
Rule Name	Displays the policy's rule name, if applicable. Refer to "New Rule Page Fields" on page 422 for information.
Description	Displays a description of the policy, for example: Ensure password
Policy Rule Exception	Displays the policy rule exception, if applicable. Refer to "New Rule Exception Page Fields" on page 430 for information.
Status	Displays the policy's status, including: • Active • Inactive • Passed • Failed
Importance	Indicates the importance of the rule that was violated, including: • Informational — Events that typically do not require a response. • Low — Events that may require a response as time permits. • Medium — Events that require a timely response, typically within 72 hours. • High — Events that require an urgent response, typically within 24 hours. • Critical — Events that require an immediate response.
Actions	You can select the following actions for each policy: • Edit Policy — Opens the Edit Policy page, where you can edit the policy. Refer to "Edit Policy Page Fields" on page 427 for information. • Edit Policy Rule — Opens the Edit Policy Rule page, where you can edit the policy's rule. Refer to "New Rule Page Fields" on page 422 for information.

Servers Page Fields

The Servers page displays the name of each server that is connected to the device on which you are displaying details. If you click a server's hostname, the Server Detail page opens. For detailed information on using SA, refer to the *HP Server Automation User's Guide*.

Keep in mind that NA only infers the location of Layer 1 wiring. NA's reduction algorithm reduces (as best it can) all connections between devices and/or servers.

Note: If you are not logged in to HP Server Automation (SA) Command Center, you are prompted to login when you click a server's hostname.

Field	Description/Action
Network Device Interface	The network device interface used by the server, for example FastEtherner1/0.
Server Host Name	Displays the server's host name. Clicking the server's hostname opens the Server Detail page. Refer to the *HP Server Automation User's Guide* for information.
Server Interface	The server interface name as reported by the operating system.
Customer	Displays the customer name.
Facility	Displays the customer's facility.
Server Use	Displays server use. Refer to the *HP Server Automation User's Guide* for information.
Deployment Stage	Displays the Deployment Stage. Refer to the *HP Server Automation User's Guide* for information.

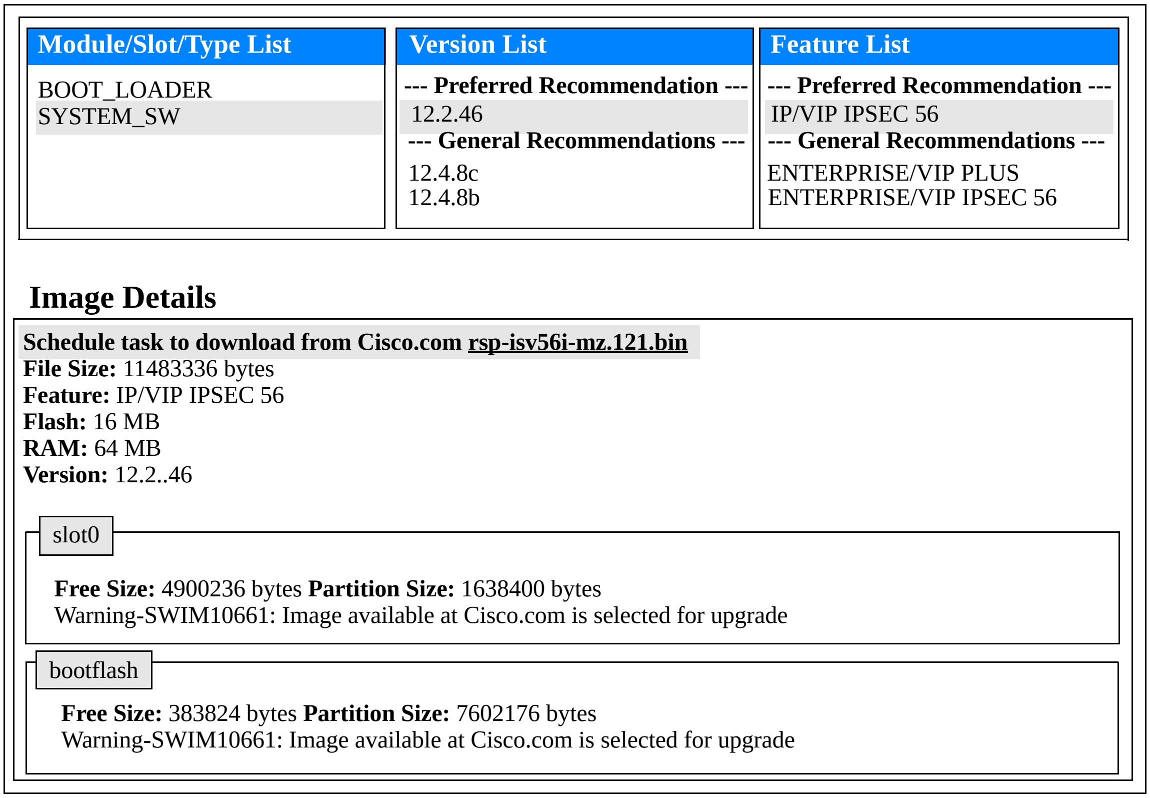
Device Software Image Recommendation Page Fields

The Device Software Image Recommendations page display software images that are available from Cisco.com, along with preferred recommendations. Attributes about the software images are also shown on the page, along with information on the location of the software image. Software images are downloaded from Cisco.com directly to the NA software repository and an image set is created.

You can apply recommendation filters on the My Preference page. Refer to "My Preference Page Fields" on page 264 for information.

Note: To review a list of Cisco supported devices, refer to the following URL. Keep in mind that NA uses data from Resource Manager Essentials (RME). As a result, the device must be supported by Cisco or you will not be able to download Cisco software images. http://cisco.com/en/US/products/sw/cscowork/ps2425/products_device_support_table09186a008086099b.html

The following figure shows a sample section of the Device Software Image Recommendation page. In the example, the shaded options have been selected. If you click the software image to download in the Image Details section, in this case *rsp-isv56i-mz.121.bin*, the software image is downloaded to the NA repository.


Module/Slot/Type List
BOOT_LOADER
SYSTEM_SW
Version List
--- Preferred Recommendation ---
12.2.46
--- General Recommendations ---
12.4.8c
12.4.8b
Feature List
--- Preferred Recommendation ---
IP/VIP IPSEC 56
--- General Recommendations ---
ENTERPRISE/VIP PLUS
ENTERPRISE/VIP IPSEC 56
Image Details
slot0
bootflash

Schedule task to download from Cisco.com rsp-isv56i-mz.121.bin
File Size: 11483336 bytes
Feature: IP/VIP IPSEC 56
Flash: 16 MB
RAM: 64 MB
Version: 12.2..46

Free Size: 4900236 bytes **Partition Size:** 1638400 bytes
Warning-SWIM10661: Image available at Cisco.com is selected for upgrade

Free Size: 383824 bytes **Partition Size:** 7602176 bytes
Warning-SWIM10661: Image available at Cisco.com is selected for upgrade

To open the Device Software Image Recommendation page:

1. Select a Cisco device that supports OS Analysis. The Device Details page opens for the device.
2. From the View menu, select Device Detail and click Software Upgrade Recommendation.

Field	Description/Action
Hostname	Displays the device's hostname. Clicking the device's hostname opens the Device Details page, where you can view information about the device.
Device IP	Displays the device's IP address. Clicking the device's IP address opens the Device Details page, where you can view information about the device.
Last Access Time	Displays the date and time the device was last accessed (such as taking a snapshot).
Last Snapshot Result	Displays the status of the last snapshot of the device's configuration. If the snapshot failed, there is a link to the Task Result page.
View menu	Opens the View menu. Refer to "View Menu Options" on page 203 for information.
Edit menu	Opens the Edit menu. Refer to "Edit Menu Options" on page 232 for information.
Provision menu	Opens the provision menu. Refer to "Provision Menu Options" on page 241 for information.
Connect menu	Opens the Connect menu. Refer to "Connect Menu Options" on page 243 for information.
Downloading Software Images	The following sections are populated with data as you select them. Refer to the above figure for a sample display. • Module/Slot/Type List — Displays BOOT_LOADER (a small program that loads software to start the operating system) and SYSTEM_SW. • Version List — When you select either BOOT_LOADER or SYSTEM_SW, a list of software image versions is displayed. • Feature List — When you select a software image version, a list of features for the software image version is displayed. When you select a feature, the Image Details section is populated with data. For software images not in the NA software repository, you can download the software image directly from Cisco.com by clicking the software image name. If the image already exists in the NA software repository, click the Software Image link. The Upgrade Device Software Task page opens, where you can upgrade the device with the selected software image. Refer to "Update Device Software Task Page Fields" on page 325 for information.
Image Details	Displays information about the software image, including the file size, version status, flash, and so on. Information on the device's slot and bootflash, along with any warnings are also displayed.

Device Tasks Page Fields

The Device Tasks page lists of all tasks associated with the device. You can also view details about the task or rerun the task from this page.

Field	Description/Action
Refresh this page every 60 seconds	Uncheck this box if you do not want the display to refresh every 60 seconds. Refer to "User Interface Page Fields" on page 63 for information on setting this value.
Check Boxes	You can use the left-side check boxes to delete selected tasks. Once you have selected the tasks, click the Actions drop-down menu and click Delete. The adjacent Select drop-down menu enables you to select or deselect all of the tasks.
Scheduled Date	Displays the date and time the task ran or is scheduled to run.
Task Name	Clicking the task name opens the Task Information page, where you can view task details, such the originator of the task, when the task was created, and the devices affected by the task. You can also view detailed task history information.
Task Status	Displays the status of the task. Statuses include: • Succeeded — The task succeeded. • Failed — The task failed. • Duplicate — The task duplicated another task, therefore it did not run. • Skipped — The task was skipped because an identical task was already running when the time arrived for this task to run. • Warning — A group task containing some failed sub-tasks, but not all tasks failed.
Priority	Displays the task's priority. There are five task priority levels, 1 through 5. 1 is the highest task priority level. Refer to "Scheduling Tasks" on page 280 for more information.
Scheduled By	Displays the login name of the person who scheduled the task (or the last user to modify the task).
Comments	Displays comments about the task.
Actions	You can select the following actions for each task: • Detail — Opens the Task Detail page, where you can view details about the task. • Run Again — Opens the Edit Task page, where you can edit and rerun a task. This link appears only when you can rerun the task.

Device Relationships Page Fields

The Device Relationships page enables you to view parent, peer, and child device relationships. In general, device relationships maintain data for both parent, peer and child devices.

Device dependencies are defined by the Device Relationships API. For example, if two devices are defined in an context relationship, the relationship is maintained by the Context Management functionality. Refer to "Add Device Context Task Page Fields" on page 361 for information on Context Management. For information on the Device Relationship API, see the *NA CLI/API Command Reference*.

Any two devices that are related will participate in what is called a device relationship. For example, if a device can only be reached through another device, the first device becomes the child and the second device becomes the parent. As a result, if the parent device is not accessible, the child device cannot be accessed.

Currently, NA only supports the VMware ESX server in terms of device relationships. Keep in mind that the CLI is used to access the VMware ESX server. However, once in the server shell, the VMware ESX server looks very similar to other Linux servers.

Once a VMware ESX server is identified, information about the server is provided from the Modules option from the Device Details menu to new devices. Refer to "Device Details Page Fields" on page 195.

These new devices will in turn be able to access their information by using information they have via their parent. In this case, a vSwitch knows it is run by a VMware ESX server. As a result, when a snapshot task is run, the vSwitch is accessed using information known about the VMware ESX server. This could mean a direct connection to the VMware ESX server or it could mean a direct connection to the device. Wherever possible, the device(s) contained in the parent are displayed as real devices.

To open the Device Relationships page, on the Device Details page, from the View menu click Device Relationships.

Field	Description/Action
Parent Devices	Displays the parent devices.
Peer Devices	Displays the peer devices
Child Devices	Displays the child devices.

To add or remove a parent, peer, or child device, click the Add or Delete link in the appropriate column. For information on adding devices, refer to "Adding Devices" on page 108.

For devices that support contexts, the following information is displayed on the Device Context page:

- Hostname of the context
- Context name
- Link to remove the context
- Link to add a new Context. Refer to "Add Device Context Task Page Fields" on page 361 for information.

Note: Specific information needed to add/remove a context is embedded in the driver (i.e., which variables are needed). These variables are presented in the Add/Remove task pages.

Device Software History Page Fields

The Device Software History page enables you to view what software is currently loaded on a device.

Field	Description/Action
Hostname	Displays the device's hostname. Clicking the device's hostname opens the Device Details page, where you can view information about the device.
Device IP	Displays the device's IP address. Clicking the device's IP address opens the Device Details page, where you can view information about the device.
Last Access Time	Displays the date and time the device was last accessed (such as taking a snapshot).
Last Snapshot Result	Displays the status of the last snapshot of the device's configuration. If the snapshot failed, there is a link to the Task Result page.
View menu	Opens the View menu. Refer to "View Menu Options" on page 203 for information.
Edit menu	Opens the Edit menu. Refer to "Edit Menu Options" on page 232 for information.
Provision menu	Opens the Provision menu. Refer to "Provision Menu Options" on page 241 for information.
Connect menu	Opens the Connect menu. Refer to "Connect Menu Options" on page 243 for information.
Change Date	Displays the date and time the software was last deployed.
Changed By	Displays the name of the person who last deployed the software to the device.
Change To	Displays the current software version running on the device.
Device Software Version	Displays the current software version running on the device.
Changed From	Displays the software version that was running on the device prior to the software deployment.
Software Level	Displays the software level rating. Refer to "Adding New Software Levels" on page 435 for more information.
Image Set	Displays the name of the last Image Set deployed to the device. An image set is a grouping of images that can be deployed to a device simultaneously. An image set can contains one or more images.

Device Sessions Page Fields

The Device Session page lists the Telnet and SSH sessions associated with the device. Sessions can include only the commands or the keystroke logging for the entire session.

Field	Description/Action
Start Date	Displays the date the session began.
Status	Displays if the session is Open or Closed.
Type	Displays if the session is via Telnet or SSH.
End Date	Displays the date the session ended.
Created By	Displays the login name of the person who opened the session.
Actions	You can select the following actions for each session: • View Full Telnet/SSH Session — Opens the Telnet/SSH Session page, where you can view the commands and system responses for that session. There is also a text display for the configuration (if any) created by this session. • View Commands Only — Opens the Telnet/SSH Session page, but limits the display to only the commands entered during the session. This can be useful when you want to create a script from the commands.

Edit Menu Options

Menu Option	Description/Action
Take Snapshot	Opens the New Task - Snapshot page. The Snapshot task enables you to schedule a snapshot. A snapshot refreshes the copy of the device configuration and related data stored in the NA database. Specifically, a snapshot checks whether the stored configuration matches the running configuration on the device. If not, the snapshot task replaces the copy of the device configuration and related data stored in the NA database. Refer to "Take Snapshot Task Page Fields" on page 317 for more information.
Discover Driver	Opens the New Task - Discover Task page. Driver discovery creates a task to check whether a driver is assigned to the device. If not, discovery overwrites the current driver with the most appropriate driver in the NA database. (**Note**: NA requires a driver to communicate with each device.) Refer to "Discover Driver Task Page Fields" on page 295 for information.
Edit & Deploy Configuration	Opens the Edit Configuration page with the current configuration, where you can edit the configuration and then deploy it. When you click the "Deploy to Device" option, you can schedule a configuration deployment or initiate an immediate configuration deployment. NA will deploy the configuration change to the device and capture the resulting configuration. The Task Result page for this task will automatically refresh while the task runs. Refer to "Deploy Config Task Page Fields" on page 183 for information.
Edit Inline Configuration Comments	Opens the Edit Configuration page, where you can enter comments, often times prefixed with two exclamation points (!!). Keep in mind that the persistent comment character is only two characters. However, some devices use multiple comment characters as delimiters. This can cause the comment engine to have difficulties parsing persistent comments.
Edit Device	Opens the Edit Device page, where you can edit the information for the device. Refer to "Edit Device Page Fields" on page 113 for information.
Edit Managed IP Addresses	Opens the Device Managed IP Addresses page, where you can view and modify all IP addresses information that might be used to access the device. Keep in mind that there must be one primary IP address that uniquely identifies each device. However, you can add alternate IP addresses to increase the odds that NA can connect to the device. Alternate IP addresses reduce administration overhead and increase the quality of device data. (**Note**: If NA fails to access a device by the primary IP address, it tries the alternate addresses in the order listed. To ensure network efficiency, move the IP addresses that are most likely to be accessed to the top of the list.) Refer to "Device Managed IP Addresses Page Fields" on page 234 for information.
Activate/Deactivate Device	Manages or unmanages the device.
Delete Device	Opens a dialog box, where you can confirm that you want to remove the device entirely from the NA database. If you permanently delete a device from the NA database, you will lose the configuration history for that device. Instead, consider editing the device to make it inactive, which preserves the configuration history.

Menu Option	Description/Action
Save As New Device	Enables you to use existing devices to pre-fill the Add Device and Add Device Template pages with the following information: • Groups • Drivers • Password information • Connection information • Model • Vendor Refer to "New Device Page Fields" on page 108 for information.
Save As New Template	Enables you to use existing devices to pre-fill the Add Device Template page with the following information: • Configuration file • Drivers • Connection information • Model • Vendor • Hierarchy Layer Refer to "Device Template Page Fields" on page 120 for information.
New Message	Opens the New Message page, where you can post a message to all NA users referring to this device. You can also track the event using SingleView. Refer to "Consolidated View of Events (SingleView)" on page 552 for information.
Process Automation	Opens the HP Operations Orchestration login page, where you can login to HP Operations Orchestration and launch HP Operations Orchestration flows in guided mode. Refer to "User Authentication" on page 75 for information on configuring HP Operations Orchestration user authentication. For information on how to use HP Operations Orchestration, refer to the *HP Operations Orchestration User's Guide*.

Device Managed IP Addresses Page Fields

The Device Managed IP Addresses page enables you to view and manage all IP addresses that might be used to access the device. Keep in mind that there must be one primary IP address that uniquely identifies each device.

You can connect to a device using:

- A primary IP address
- Any number of secondary IP addresses (provided by the device or manually entered)
- A console server IP address and port
- A Bastion Host
- Hop Boxes
- IP address of another device

Field	**Description/Action**
Define Bastion Host link	If the device does not have a Bastion Host defined, the New IP Address page opens. Refer to "New IP Address Page (Bastion Host)" on page 236 for information. If the device does have a Bastion Host defined, two additional links are displayed: • Edit Bastion Host • Delete Bastion Host
New IP Address link	Opens the New IP Address page. Refer to "New IP Address Page (Custom IP Address)" on page 237 for information. It is recommended that when using NAT or other addressing schemes, you add IP addresses that are not automatically detected by NA. The IP addresses you add here are labeled "custom".
New Console Server link	Opens the New IP Address page. Refer to "New IP Address Page (Console Server)" on page 238 for information.
New Hop Box link	Opens the New IP Address page. Refer to "New IP Address Page (Hop Box)" on page 239 for information.
New Connection Through link	Opens the New IP Address page. Refer to "New IP Address Page (New Connection Through)" on page 240 for information.
Reset last used IP link	Enables you to reset the last used IP address.
Port IP	Displays the device's port IP address, either Primary, Alternate, or Custom. (All IP Addresses populated by parsing the device configuration are listed as "Alternate".)
Use To Access Device	Displays No or Yes. NA tries to access the device first by its primary IP address, then by its console server address (if any), and finally by any alternate IP addresses that states Yes in this field (No is the default).
Type	Displays the type of IP address: Primary, Alternate, or Custom. The IP Address from the New/Edit Device page is always the primary IP address. Additional IP addresses detected are alternate addresses. If IP addresses are added using the New IP Address link, they are considered custom IP addresses.

Field	Description/Action
Realm Name	Displays the Realm name. The Realm name is returned from the Gateway. The Realm name is set when the Gateway is install and cannot be modified in NA.
Actions	You can select the following actions for each device: • Edit — Opens the Edit Device page for the primary IP Address, where you can modify the IP address and subnet mask, insert the new IP address before the primary IP address for a new access order, and comment the change. This page is displayed for the Alternate, NAT, TFTP Server, and Custom IP Addresses. Refer to the “Edit Device Page Fields” on page 113 for information. Note that only those IP addresses that were manually added to the device can be selected for deletion. For all other IP Addresses, the New IP Address page opens. Refer to the “New IP Address Page (Custom IP Address)” on page 237. • Move Up — When multiple alternate IP addresses appear in the list, this option moves the IP address up in the list. NA tries the alternate addresses in the order listed. (**Note**: This option is only available for Secondary, Custom, and Hop Box IP Addresses. Primary and Console IP Addresses are not sortable.) • Move Down — When multiple alternate IP addresses appear in the list, this option moves the IP address down in the list. NA tries the alternate addresses in the order listed. (**Note**: This option is only available for Secondary, Custom, and Hop Box IP Addresses. Primary and Console IP Addresses are not sortable.)

New IP Address Page (Bastion Host)

On the Device Managed IP Addresses page, when you click the Define Bastion Host link, the New IP Address page opens. Note that Bastion host can be used on Linux or Solaris systems.

Note: When configuring a Bastion Host, all attempts to access the device (including Console Server access) will first login to an intermediary host (called a “Bastion Host”), and then attempt to connect to the device.

Field	Description/Action
Bastion Host IP Address Value	Enter the IP Address of the Bastion Host. Note that you can enter a Hostname and NA will resolve it to an IP Address.
Username	Enter the username to use for accessing the Bastion Host.
Password	Enter the password to use for accessing the Bastion Host.
Confirm Password	Re-enter the password for confirmation.
Device Connection Method	Enter the method to access the device once logged in to the Bastion Host, either SSH or Telnet.
Connection Script Variables	Enter a set of variables to customize the connection scripting. The default prompt pattern (regular expression) to look for to identify that NA has connected into the intermediary host is: `(\x23|\x24|%)`, which translates to a '`#`' or a '`$`' or a '`%`'. (**Note**: Leaving the fields blank uses the default variables. The default variables should work for most Unix Bastion Hosts.)
Comments	Enter comments, if necessary.

New IP Address Page (Custom IP Address)

On the Device Managed IP Addresses page, when you click the New IP Address link, the New IP Address page opens.

Field	Description/Action
Custom IP Address Value	Enter a new IP Address. Note that you can enter a Hostname and NA will resolve it to an IP Address.
Device Access	Device access enables you to use the custom IP address to access the device. Select one of the following options: • No — The IP address will not be used to access the device. • Yes — The IP address will be used to access the device. • Only — Only use this IP address (path) to access the device. Device access for all other devices is set to No.
Comments	Enter comments, if necessary.

New IP Address Page (Console Server)

On the Device Managed IP Addresses page, when you click the New Console Server link, the New IP Address page opens.

Note: Console server is used when a Telnet-enabled console server provides an automatic pass-through to a device based on a port. This option only works for Telnet. Enabling a console server automatically enables Telnet for the device.

Field	Description/Action
Console IP Address Value	Enter a new console IP Address. Note that you can enter a Hostname and NA will resolve this to an IP Address.
Console Port	Enter a Console Port on the Console Server.
Device Access	Device access enables you to use the console server to access the device. Select one of the following options: • No — The IP address will not be used to access the device. • Yes — The IP address will be used to access the device. • Only — Only use this IP address (path) to access the device. Device access for all other devices is set to No.
Comments	Enter comments, if necessary.

New IP Address Page (Hop Box)

On the Device Managed IP Addresses page, when you click the New Hop Box link, the New IP Address page opens.

Hop Box is a general use of the “Bastion Host” scripting to connect to a device. Unlike the Bastion Host, the Hop Box option requires you to specify the IP address to use once logged into the intermediary host. Hop Box paths do not first go through the specified Bastion Host (if any).

Field	Description/Action
Hop Box IP Address Value	Enter the IP Address of the Hop Box. Note that you can enter a Hostname and NA will resolve this to an IP Address.
Target IP (from Hop Box)	Enter the IP Address to jump to from the Hop Box.
Username	Enter the username to use for accessing the Hop Box.
Password	Enter the password to use for accessing the Hop Box.
Confirm Password	Re-enter the password for confirmation.
Device Connection Method	Enter the method to access the device once logged-in to the Hop Box, either SSH or Telnet.
Connection Script Variables	Enter a set of variables to customize the connection scripting. The default prompt pattern (regular expression) to look for to identify that NA has connected into the intermediary host is: `(\x23|\x24|%)`, which translates to a '`#`' or a '`$`' or a '`%`'. (**Note**: Leaving the fields blank uses the default variables. The default variables should work for most Unix Bastion Hosts.)
Comments	Enter comments, if necessary.

New IP Address Page (New Connection Through)

On the Device Managed IP Addresses page, when you click the New Connection Through link, the New IP Address page opens.

The New Connection Through option enables you to connect to a device through another device. Keep in mind that this option is only supported via the CLI. SNMP is not supported.

Note: New Connection Through can only be used for devices already in NA.

Using Telnet and SSH, there are four possible combinations:

- Access Device A (SSH) through Device B (SSH)
- Access Device A (SSH) through Device B (Telnet)
- Access Device A (Telnet) through Device B (SSH)
- Access Device A (Telnet) through Device B (Telnet)

As a result, when connecting Device A through Device B, New Connection Through automatically adds Device B. As part of the NA Module Status diagnostic, any contexts found are automatically added as devices and will have connection paths automatically configured. Refer to "Add Device Context Task Page Fields" on page 361 for information on device contexts.

Field	Description/Action
Connection Through IP Address Value	Enter a new IP Address for which to connect through.
Device Access	Device access enables you to use the IP address to access the device. Note that SCP is not available. Select one of the following options: • No — The IP address will not be used to access the device. • Yes — The IP address will be used to access the device. • Only — Only use this IP address (path) to access the device. Device access for all other devices is set to No.
Comments	Enter comments, if necessary.

Provision Menu Options

Menu Option	Description/Action
Provision Device from Template	Opens the Device Template page where you can view Device Templates for this device. Refer to "Device Template Page Fields" on page 120 for information.
Check Policy Compliance	Opens the New Task - Check Policy Compliance page, where you can view devices whose configurations and software are or are not in compliance with current policies. Refer to "Check Policy Compliance Task Page Fields" on page 374.
Configure Syslog	Opens the New Task - Configure Syslog page, where you configure Syslog on this device for real-time change detection. Refer to "Configure Syslog Task Page Fields" on page 286.
Delete ACLs	Opens the New Task - Delete ACLs page, where you can delete ACLs. Refer to "Deleting ACLs" on page 697.
Deploy Passwords	Opens the New Task - Deploy Passwords page, where you can setup a task to deploy password changes to the device. Refer to "Deploy Passwords Task Page Fields" on page 290.
Reboot Device	Opens the New Task - Reboot Device page, where you can Reboot Devices that are in the NA database. Refer to "Reboot Device Task Page Fields" on page 298.
Run ICMP Test	Opens the New Task - Run ICMP Test page, where you can schedule either a ping or traceroute test from a device to one or more devices. Refer to "Run ICMP Test Task Page Fields" on page 301.
Run Command Script	Opens the New Task - Run Command Scripts page, where you can edit and schedule a command script for the device. Refer to "Run Command Script Task Page Fields" on page 306.
Run Diagnostics	Opens the New Task - Run Diagnostics page, where you can schedule diagnostics for the device. Refer to "Run Diagnostics Task Page Fields" on page 312.
Synchronize Startup and Running	Opens the New Task - Synchronize Startup and Running page, where you can synchronize the startup and running of configurations for a device. Refer to "Synchronize Startup and Running Task Page Fields" on page 321.
Update Device Software	Opens the New Task - Update Device Software page, where you can schedule the deployment of software to one or more devices. Refer to "Update Device Software Task Page Fields" on page 325.
New VLAN	Opens the New Task - VLAN page, where you can configure VLANs on a network switch. Refer to "VLAN Task Page Fields" on page 365 for information.
OS Analysis	Opens the New Task - OS Analysis Task page that collects data about the Cisco devices, such as Information about the sysoid (unique identifier for device model), OS version, flash storage options, modules, and so on. Refer to "OS Analysis Task Page Fields" on page 352 for information.
Device Contexts	Opens the New Task - Device Context page where you can create a device context. A context is a device inside a device. A context can be hardware (with modules and slots) or virtual. NA uses device contexts to automatically add a relationship between a parent device and a child device. NA does not require a context to have an IP address. Rather, you can configure a through path connection to the context, thereby enabling NA to manage the context. Refer to "Add Device Context Task Page Fields" on page 361 for information.

Menu Option	Description/Action
Port Scan	Opens the New Task - Port Scan Task page that enables Nmap to discover network devices. Nmap can also be used to scan a device's ports and return details on which ports are open and what services they provide. Refer to "Port Scan Page Fields" on page 355 for information.

Connect Menu Options

NA supports single sign-on to network devices using the Telnet or SSH protocol. The NA server acts as a Telnet/SSH proxy. The data transferred is in clear text format.

Keep in mind that if you do not use the NA server as a Telnet/SSH proxy, you can login directly to the device through a secured URL or by using standard Telnet commands.

Menu Option	Description/Action
Via Proxy Using Telnet	Opens a Telnet window, where you can enter Telnet commands to this device.
Via Proxy Using SSH	Opens an SSH window, where you can enter SSH commands to this device.

Chapter 6: Managing Users

Use the following table to quickly locate information.

Topic	Refer to:
Adding Users	“Adding Users” on page 246
Email Notification	“Email Notification” on page 248
Configuring User Passwords	“Configuring User Passwords” on page 252
Adding User Groups	“Adding User Groups” on page 255
Adding New User Roles	“Adding User Roles” on page 259
Editing User Settings	“Editing User Settings” on page 262
Quick Launches	“What is Quick Launch?” on page 267
Customizing the NA Home Page	“Customizing the NA Home Page” on page 271
Search/Connect Function	“Search/Connect Function” on page 275

Adding Users

Designing user authentication and authorization is a challenging task. The choices you make affect how HP Network Automation (NA) is used. Adopting a proper authentication and authorization design helps alleviate many security risks.

Best practices in both information security and IT departments generally include the concept of “least privilege”, which means that each user should be assigned the least amount of rights necessary to perform their job duties. In addition, the nature of some organizations creates an environment where it is appropriate for the tasks that each user can perform to be separated by each user’s role.

The following terms are used in this section:

- Role — Roles are used to partition users into groups that share the same security privileges. A user assigned to a role is granted permissions defined by the role. For example, if a user is authorized to perform certain operations, such as adding devices, managing configuration policies, or deploying software, NA uses fixed role identities with which to access resources. Creating a new user role from scratch, rather than using an existing role as a starting point, creates a template with default deny permissions on every action type. This allows roles to be easily created in line with the “least privilege” security best practice.
- User Group — A user group is a logical container for the purpose of user management. The System Administrator can assign users to user groups, which in turn map to specific roles. Keep in mind that a user group can be assigned one or more roles.

To add a new user, on the menu bar under Admin click Users. The All Users page opens. Click the New User link at the top of the page. The New User page opens. Refer to “New User Page Fields” on page 249.

Note: You can also navigate to the New User page by clicking the New User option under Admin.

Note: You can import new users and modifications to existing users from a CSV file. For more information, see “Import Users Task Page Fields” on page 336.

All Users Page Fields

Field	Description
New User link	Opens the New User page, where you can add users. Refer to “New User Page Fields” on page 249 for information. Keep in mind that only the System Administrator can add users.
Search for Users link	Opens the Search For Users page, where you can search for users by first name, last name, email address, and/or AAA user name. Refer to “Searching for Users” on page 525 for information.

Field	Description
Logged on Users link	Opens the Logged On Users page, where you can view who is currently logged in, including their user name, user host, and the last access time. Keep in mind that this only shows users who are logged in using the Web UI, not the Command Line Interface (CLI). (**Note**: You can also select the Logged On Users option from the Admin drop-down menu to view this page.) Refer to “Logged on Users Page Fields” on page 248 to for information.
User Groups link	Opens the User Groups page, where you can add and edit user groups. Refer to “User Groups Page Fields” on page 255 for information.
User Roles & Permissions link	Opens the User Roles & Permissions page, where you can edit user permissions. Refer to “User Roles & Permissions Page Fields” on page 259 for information.
Users in this group	Displays the following icons: • 👤 Regular User Account • 👤 Disabled User Account
User Name	Displays the user’s full name.
First Name	Displays the user’s first name.
Last Name	Displays the user’s last name.
Email	Displays the user’s email address.
Actions	You can select the following options: • Edit — Opens the Edit User page. If the account is your own account, the My Profile page opens. Note that only users in the Administrator Group can view password options on the My Profile page. Refer to “My Profile Page Fields” on page 262 for information. Any changes to your profile are shown on the User List page. • Delete —You can delete a user (with Admin privileges). • Permissions — Opens the User Permissions page. If you click the Edit User Profile option at the top of the page, the Edit User page opens. You can make changes to the user profile and click Save. The changes are shown on the User List page. Refer to “New User Page Fields” on page 249 for information. • Config Changes — Opens the Config Search Results page. This page displays what configuration changes, if any, the user made. Refer to “Viewing Device Configuration Changes” on page 174 for information.

Logged on Users Page Fields

The Logged on Users page enables you to view who is currently logged in to NA, including their user name, email address, user's host system, and the last date and time the user accessed the host system. Keep in mind that this page only shows users who are logged in using the NA UI, not the Command Line Interface (CLI).

Field	**Description/Action**
User Name	Displays the user's name
Email Address	Displays the user's email address. To send and receive email messages to logged-in users, refer to "Email Notification" on page 248.
User Host	Displays the host IP address of the system to which the user is logged in.
Last Access Time	Displays the date and time the user last accessed the system.

Email Notification

While logged-in to NA, you can send messages to one or more logged-in NA users. Keep in mind that while you can delete your messages, once you logout of NA, all messages are automatically deleted.

Note: You cannot use the API to implement this feature because the NA UI framework communicates the message. There is no database access.

To send a message:

1. From the Admin menu, click Logged On Users. The Logged On Users page opens.
2. Check the checkboxes of the user(s) to whom you want to send a message. Note that you can select all users from the Select drop-down menu.
3. From the Actions drop-down menu, select Send Message. The Send Message page opens.
4. Enter your message text in the Message field.
5. When you are finished entering your message text, click the Submit button. If successful, "Your message has been sent." is displayed at the top of the Logged On Users page.

To read a message:

1. If you have a new message, click the "A new message has arrived" link at the top of the left-hand frame of the NA UI. The message is displayed, including who sent the message and when it was sent. You have the option of relying to the message or deleting it.

   Note: The "A new message has arrived" link changes to "View Messages" after you have read all of your messages. All messages are displayed in the order that they were sent.

2. If you click the Reply button, the Send Message page opens, enabling you to reply to the message. If you click the Delete button, the message is deleted.

When sending a reply, NA uses the UserID from the original message's Sender UserID. You are automatically the SenderID of the new message.

1. Select the Reply button under the message. The Send Message page opens.
2. Enter your message text and click the Submit button. The “A new message has arrived” link is displayed at the top of the left-hand frame of the NA UI for the user to whom you sent the message.

New User Page Fields

When you are first adding users, this page is empty except for your Admin account information. After you have completed this page and saved it, if you need to edit the information, you can do so on the Edit User page. The fields on the Edit User page are identical to the fields on the New User page.

Field	**Description/Action**
User Information	
User Name	Enter the NA user name of the user. This name is used to login to NA, such as Operator or Administrator. **Note**: User names can contain alphanumeric characters, periods (.), underscores (_), hyphens (-), and backslashes(\) only.
Password	Enter the NA password for the user. This is the password used when logging into NA. Refer to “Configuring User Passwords” on page 252 for information on setting passwords.
Confirm Password	Enter the user’s NA password for confirmation.
Password Option	Select one or more of the following options: • User must change password at next login • User cannot change password • Password never expires • Account is locked out Refer to “Configuring User Passwords” on page 252 for information on setting password options.
First Name	Enter the first name of the user.
Last Name	Enter the last name of the user.
Email Address	Enter the email address of the user.

Field	Description/Action
User belongs to selected groups	Select one or more of the following default user groups to which the user belongs. These groups provide user roles and all associated permissions for the user. Keep in mind that NA does not assign a group by default. A user that does not belong to a group can only perform limited tasks, such as viewing devices and configuration changes. (**Note**: If you created a new group, it is displayed in the list.) • Limited Access User — Limited Access users are typically operators that do not have passwords to configure network devices. While they have permission to view devices, they cannot modify most information in the NA database, or run batch operations or operations which would reconfigure network devices. • Full Access User — Full Access users are typically network engineers trusted with passwords to configure some, if not all, devices in the network. They have permission to modify most information in the NA database, and can reconfigure devices one-at-a-time, but not in batch mode. Often times they are restricted as to which devices they have permission to reconfigure. • Power User — Power users are typically expert engineers allowed to perform most actions. They can reconfigure and otherwise act on groups of devices. • Administrator — Administrators are responsible for administering NA, including managing users, setting policy, and running network-wide operations. They have permission to take any action on any device. • View All Partitions — Enables users to view all Partitions. A Partition is a set of NA devices. Each Partition belongs to only one NA Core. As a result, a Partition is managed by one (and only one) NA Core. In addition, each device belongs to one and only one Partition. Refer to “Segmenting Devices and Users” on page 150 for information on configuring Partitions.
Site	Select the partition to which this user belongs. The user will only be visible to other users who have view permission to that partition. **Note**: The Site drop-down menu is not available if the user has access to only one partition.
Status	Select one of the following options: • Enabled — The account is enabled (the default). • Disabled — The account is disabled. You can use this option to disable an account while still keeping the account on the system.
External Auth Failover	If external authentication server cannot be reached, you can enable authentication failover to local authentication.
Comments	Enter comments about the account.
AAA	
AAA User Name	Enter the AAA (TACACS+ or RADIUS) username for this user. This enables NA to associate AAA usernames with NA usernames. Keep in mind if you want NA to failover to local authentication, you must enable this capability on the user’s account. By default, NA will not failover to local authentication.
AAA Password	Enter the AAA password for this user.
Confirm AAA Password	Enter the AAA password again for verification.

Field	Description/Action
Use AAA Login for Proxy Interface check box	If checked, NA checks the user’s AAA credentials when logging the user into the Telnet/SSH Proxy.
SecurID	
After a new user has been added, a link to the Manage Software Tokens page is displayed when you edit the user's information. The Manage Software Tokens page enables you to add Software Token licenses associated with the user's login. Refer to “Adding SecurID Software Tokens” on page 636.	

Configuring User Passwords

The following options are displayed on the New and Edit User pages for NA users with user password setting permissions for creating new user profiles or editing existing user profiles:

- User must change password at next logon
- User cannot change password
- Password never expires
- Account is locked out

These options are also shown on the My Profile page if the user is included in the Administrator Group. Refer to "My Profile Page Fields" on page 262 for information.

Note: When using the CLI, users will not be able to login if their passwords have expired. They must reset their password using the NA UI.

User Scenario One

User A is leaving the company to pursue other opportunities and there is a need to disable his account yet preserve historical data related to the account. The NA system administrator:

1. Logs in to NA.
2. From the main menu under Admin, the NA system administrator clicks the Users option. The All Users page opens.
3. The NA system administrator clicks the Edit option in the Actions column for User A. The Edit User page opens for User A.
4. On the Edit User page, the NA system administrator selects the "Disabled" option in the Status field and clicks the Save button.

As a result of the above action, if User A were to attempt to login to NA, he receives the following message: `Account is disabled`.

User Scenario Two

The NA system administrator is about to do maintenance on the NA system. He needs to ensure that there are no NA users logged into the system. After everyone has logged out of NA, the NA system administrator:

1. Logs in to NA.
2. From the main menu under Admin, the NA system administrator clicks the Users option. The All Users page opens.
3. The NA system administrator clicks the Edit option in the Actions column for each user. The Edit User page opens.
4. On the Edit User page, the NA system administrator selects the “Account locked out” checkbox in the Password Options field and clicks the Save button.

As a result of the above action, if any user attempts to login to NA during the system maintenance period, he/she receives the following message: `Account is locked out.`

After completing system maintenance, the NA system administrator returns to the Edit User page for each user and unchecks the “Account is locked out” checkbox and clicks the Save button. As a result, users can now login to NA.

Note: Currently, there is no way to batch edit user accounts.

User Scenario Three

User B has been on vacation for several weeks. While she was away, the NA system administrator was told to comply with the new corporate password policy. Employees must now change their NA passwords every 30 days. To comply with this new policy, the NA system administrator:

1. Logs in to NA.
2. From the main menu under Admin, the NA system administrator clicks the Users option. The All Users page opens.
3. The NA system administrator clicks the Edit option in the Actions column for User B. The Edit User page opens.
4. On the Edit User page, the NA system administrator selects the “User must change password at next logon” checkbox in the Password Options field and clicks the Save button.

As a result of the above action, when User B arrives at work and tries to login to NA, she receives the following message: `Your password has expired. Please reset your password. Your new password must be different from your previous <eight> passwords.`

User B must enter her user name, old password, new password, and then enter her new password again for confirmation.

Note: You can change your password on the Change Password page, unless the NA system administrator has checked the “User cannot change password” option on the New or Edit User page. Refer to “Change Password Page Fields” on page 267 for information.

Password Expiration

NA system administrators can enable or disable NA user password expiration by selecting the “Password never expires” option on the New and Edit User pages. For security, the following settings are included in the *appserver.rcx* file:

- *security/user_password_expiration_enabled* — By default, this setting is false.
- *security/user_password_expire_in_days* — By default, the value is 180 days. The value must be greater than 0 and less than 1,000. This setting is ignored if the *security/user_password_expiration_enabled* setting is false.

If you need to modify the default values, do the following:

1. Stop NA.
2. Open the *$NA/adjustable_options.rcx* file and add the following entries anywhere between the `<options>` and `</options>` tags:

```
<option name=”security/user_password_expiration_enabled”>false</option>
<option name=”security/user_password_expire_in_days”>180</option>
<option name=”security/user_password_reuse_allowed”>false</option>
<option name=”security/user_password_history_size”>8</option>
```

3. Modify the values as needed and save the file.
4. Repeat Steps 1, 2, and 3 on all NA Cores.
5. Restart NA.

Password Reuse

To prevent users from using previous passwords, previous passwords are stored in the database. A new RN_PASSWORD_HISTORY table has been created for this purpose.

Two new settings are included in the *appserver.rcx* file:

- *security/user_password_reuse_allowed* — The default value is false.
- *security/user_password_history_size* — The default value is 8. The valid range is [1, 999].

Adding User Groups

To add a new user group, on the menu bar under Admin click User Groups. The User Groups page opens. Click the New User Group link at the top of the page. The New User Group page opens. Refer to "New User Group Page Fields" on page 256.

Note: You can also navigate to this page from the All Users page by clicking the User Groups link.

Note: You can import new user groups and modifications to existing user groups from a CSV file. For more information, see "Import Users Task Page Fields" on page 336.

User Groups Page Fields

Field	Description/Action
New User Group link	Opens the New User Group page, where you can add user groups. Refer to "New User Group Page Fields" on page 256 for information.
Users link	Opens the All Users page, where you can edit user groups. Refer to "All Users Page Fields" on page 246 for information.
User Roles & Permissions link	Opens the User Roles & Permissions page, where you can edit user permissions. Refer to "User Roles & Permissions Page Fields" on page 259 for information.
Group Name	Displays the name of the user group. Clicking any of the Group Name links opens User Details page, where you can view all of the current users in the group. Refer to "All Users Page Fields" on page 246 for information on adding users and editing user profiles.
Description	Displays a brief description of the group.
User Roles	Displays the user roles that have been assigned to the group. Clicking a user role opens the User Role Information page, where you can view details about the user role. Refer to "Adding User Roles" on page 259 for information.
Actions	You can select the following options: • Edit — Opens the Edit User Group page. Refer to "User Groups Page Fields" on page 255 for information. • Delete —You can delete the group (with Admin privileges). • Permissions — Opens the View Permissions page. Refer to "New User Group Page Fields" on page 256 for information.

New User Group Page Fields

By default, a user group will use the most permissive Command Permission as defined by the union of roles applied to the user group. To ensure the appropriate lock-down of permissions, assign the most restrictive roles possible to the user group.

Field	Description/Action
General Information	
Group Name	Enter the name of the user group.
Description	Enter a description of the user group.
Site	Select the partition to which this user group belongs. **Note**: The Site drop-down menu is not available if the user has access to only one partition.
Command Permissions	
Existing Command Permission Role	Users in the user group must be explicitly granted the corresponding command permission for every action they attempt to perform. If checked (the default), select one or more of the following options: • Administrator — Administrators are responsible for administering NA, including managing users, setting policy, and running network-wide operations. They have permission to take any action on any device. • Power — Power users are typically expert engineers allowed to perform most actions. They can reconfigure and otherwise act on groups of devices. • Full Access — Full Access users are typically network engineers trusted with passwords to configure some, if not all, devices in the network. They have permission to modify most information in the NA database, and can reconfigure devices individually, but not in batch mode. Often times they are restricted as to which devices they have permission to reconfigure. • Limited Access — Limited Access users are typically operators that do not have passwords to configure network devices. While they have permission to view devices, they cannot modify most information in the NA database, or run batch operations or operations which would reconfigure network devices. **Note**: If you have defined a command permission role other than the default command permission roles, it is displayed in the list.

Field	Description/Action
Customized Command Permission Role	If checked, you can customize command permission roles specific to this user group. For each command, click a button to grant or deny permission to this role. For a complete list of Command permissions, refer to "Appendix B: Command Permissions" on page 719. You can click Grant All to grant permission to all commands. This is useful for Admin users and when you want to deny permission to only a few commands. Click Deny All to deny permission to all commands. By default, all commands are denied. The following icons to the right of certain commands indicate that you may need to modify device permissions or script permissions. • Modify Device Permission required icon — NA can control permissions on a per-device basis. Modify Device Per Permission specifies whether you can modify a device. You must have Modify Device Permission for the specific device(s) you want to run this command against. See "Modify Device Permissions" below. • Script Permission required icon — NA can control permissions on a per Command Script basis. Script Permission specifies whether you can run a Command Script. You must have Script Permission for the specific Command Script you want to run. See "Script Permissions" below. **Note**: Custom scripts are presumed to modify device configurations. Therefore, they are checked against the user's Modify Device Config permissions.
Modify Device Permissions	
All Devices	Enables users in the group to modify all devices. **Note**: If a user without Modify Device permissions views a device configuration, the sensitive information in the device configuration, such as passwords and SNMP community strings, are masked. This ensures that users without Modify Device permissions cannot view sensitive data.
None	No device can be modified. This is the default setting.
Existing Modify Device Permission Role	Enables you to select existing Modify Device permission roles for the users in the group. If there are no existing roles configured, the following message is displayed: No existing roles found.
Customized Modify Device Permission Role	Enables you to select Device Permission roles from the list specific to this user group.
Script Permissions	
All Scripts	Enables the users in the group to modify all scripts.
None	No scripts can be modified. This is the default setting.
Existing Script Permission Role	Enables you to select existing Script permission roles for users in the group. If there are no existing roles configured, the following message is displayed: No existing roles found.
Customized Script Permission Role	Enables you to select one of the Script Permission roles from the list specific to this user group.
Customized Script Permission Role	Enables you to select customized Script permission roles from the list.

Field	Description/Action
View Partition Permissions	
All objects	Enables the users in the user group to view all Partitions. (Refer to “Segmenting Devices and Users” on page 150 for information.) **Note**: If you are not using View Permissions, new users are placed in the View All Partitions group, giving them View Permission to all devices. If you create View Permissions, new users are not implicitly granted any View Permissions.
None	No Partitions are viewable. This is the default setting.
Existing View Permission Role	Enables you to select an existing View permission role for users in the user group. If there are no existing roles configured, “No existing roles found” is displayed.
Customize View Permission Role	Enables you to select View permission roles from the list. If the All radio button is selected, all Partitions are included.
Users	
Users in Group/All Users	To add a user, select the user from the right-hand box and click << Add. To remove a user, select the user in the left-hand box and click Remove.

Be sure to click the Save button when you are finished.

Adding User Roles

Users must be explicitly granted the corresponding command permission for each action they want to perform, such as viewing a Web page or executing a command. A set of command permissions creates a command permission role. You can then apply the role to a user group to set the command permissions for that given user group. For example, the network operations staff could have permission to access device records and view changes, but not to script changes on devices or remove devices.

Note: If you are not using View Permissions, new users are placed in the View All Partitions group, giving them View Permission to all devices. If you create View Permissions, new users are not implicitly granted any View Permissions.

To add a new user role:

1. On the menu bar under Admin, click the User Roles & Permissions option. The User Roles & Permissions page opens.
2. Click the New User Role link at the top of the page. The New User Role page opens. Refer to "New User Role Page Fields" on page 261.

User Roles & Permissions Page Fields

Field	**Description/Action**
New User Role link	Opens the New User Role page, where you can select a user role. Refer to "New User Role Page Fields" on page 261 for information.
Users link	Opens the All Users page, where you can view current users and add new additional ones. Refer to "All Users Page Fields" on page 246 for information.
User Groups link	Opens the User Groups page, where you can view current user ground and add new additional ones. Refer to "User Groups Page Fields" on page 255 for information.
System Default Roles	
Role Name	Displays the role name. You can select any role to view information for the role, including a list of command permissions for the role.
Role Type	Displays the role type, including Command Permission, Modify Device Permission, Script Permission, and View Partition Permission.
Description	Displays a description of the role.
Actions	You can select the following options: • Edit — The Edit User Role page opens. Refer to "Adding User Roles" on page 259 for information. Keep in mind that default roles cannot be edited. • Create Copy — Opens the Edit User Role page, where you can add a new user role. Refer to "New User Role Page Fields" on page 261 for information. • Delete — You can delete the role (Admin privileges only). Keep in mind that default roles cannot be deleted.

Field	Description/Action
User Defined Roles	
Role Name	Displays the role name. You can select any role to view information for the role, including a list of command permissions for the role.
Role Type	Displays the role type, for example Command Permission, Modify Device Permission, View Partitions Permissions, and Script Permission.
Description	Displays a description of the role.
Actions	You can select the following options: • Edit — The Edit User Role page opens. Refer to "New User Role Page Fields" on page 261 for information. • Create Copy — Opens the Edit User Role page, where you can add a new user role. Refer to "New User Role Page Fields" on page 261 for information. Keep in mind that user-defined roles cannot be copied. • Delete — You can delete the role (with Admin privileges only).

New User Role Page Fields

Field	Description/Action
New User Role	Select a user role from the drop-down menu. The display is modified depending on your selection. The options include: • Command Permission — Enter the name and description of the user role. For each command, click a button to grant or deny permission to this role. For a complete list of Command permissions, refer to “Appendix B: Command Permissions” on page 719. You can click Grant All to grant permission to all commands. This is useful for Admin users and when you want to deny permission to only a few commands. Click Deny All to deny permission to all commands. • Modify Device Permission — Enter the name and description of the user role. Use the Device Selector to select the device group(s). Refer to “Device Selector” on page 144 for information on how to use the Device Selector. This role will have Modify Device permission for all devices that are members of the selected device groups. • Script Permission — Enter the name and description of the user role. Select the scripts from the list. This role will have Script permission to all selected scripts. • View Partition Permission — Enter the name and description of the user role. Select the Partitions from the list. This role will have View Partition permission for all devices and/or users that are members of the selected partition’s device and/or user groups. Keep in mind that View Partition Permissions are assigned to user groups, not individual users. Users belonging to multiple user groups can obtain multiple View Partition Permissions. For information on segmenting devices, refer to “Segmenting Devices and Users” on page 150.

Be sure to click the Save button when you are finished.

Keep in mind that user groups are not automatically assigned to user roles. To assign a user group to a user role:

1. On the menu bar under Admin, click User Groups. The User Groups page opens.
2. Click the Edit option in the Actions column for the group you want to add to the new role. The Edit User Group page opens. Refer to “New User Group Page Fields” on page 256 for information.

Editing User Settings

On the NA Home page, the “My Workspace” area includes the following sections:

- Current Device — Displays the current device, if applicable.
- Current Device Group — Displays the current device group. Inventory is the default.
- My Favorites — Displays a list of your favorite devices, URLs, and/or NA pages. You can add items to this list by clicking the Add To Favorites link at the top of most NA pages.
- Quick Launches — Refer to “What is Quick Launch?” on page 267.
- My Settings — Refer to “My Settings” on page 262 for information.

My Settings

You can select the following options under My Settings:

- My Profile — Refer to “My Profile Page Fields” on page 262.
- My Workspace — Refer to “My Workspace Page Fields” on page 264.
- My Preferences — Refer to “My Preference Page Fields” on page 264.
- My Permissions — Refer to “My Permissions Page Fields” on page 266.
- Change Password — Refer to “Change Password Page Fields” on page 267.
- Quick Launch — Refer to “What is Quick Launch?” on page 267.

My Profile Page Fields

The My Profile page enables you to change your user settings, such as your user name, password, and email address. Note that only users in the Administrator Group can view password options. Refer to “Configuring User Passwords” on page 252 for information.

On the NA Home page under My Settings click My Profile. The My Profile page opens. Be sure to click the Save button when you are finished.

Field	Description/Action
User Information	
User Name	Enter a new NA username.
Password	Enter a new NA password.
Confirm Password	Enter the new NA password again for confirmation.

Field	Description/Action
Password Option	Select one or more of the following options: • User must change password at next login • User cannot change password • Password never expires • Account is locked out Refer to "Configuring User Passwords" on page 252 for information on setting password options.
External Resource Credentials	Clicking the Make changes to your External Resource Credentials link opens the Change Password page. Refer to the "Change Password Page Fields" on page 267.
First Name	Enter a new first name.
Last Name	Enter a new last name.
Email Address	Enter a new email address.
User belongs to groups	Displays the groups to which you belong. Clicking a group opens the current list of users that belong to the group.
External Auth Failover check box	Check if in the event external authentication fails, authentication automatically fail-overs to local authentication.
Comments	Enter any comments about the user account.
AAA	
AAA User Name	Enter a new AAA (TACACS+ or RADIUS) username.
AAA Password	Enter a new AAA password.
Confirm AAA Password	Enter your new AAA password again for confirmation.
Use AAA Login for Proxy Interface check box	If checked, your AAA login information is used with each NA Telnet and SSH session.
SecurID	
Manage Software Token licenses link	NA can be configured to login to devices using SecurID credentials. Clicking this link opens the View SecurID Tokens page. Refer to "Adding SecurID Software Tokens" on page 636 for information. (**Note**: This link is not displayed if software tokens are not supported on your platform or SecurID is not properly configured.)

My Workspace Page Fields

To edit your workspace, on the NA Home page under My Settings click My Workspace. The My Workspace page opens.

Field	**Description/Action**
Favorite Links	Displays your favorite links. Links can be devices, NA pages, or other URLs. To remove a link, click the red Delete icon next to the link you want to remove. You can also rename a link by entering a new name and then clicking the Rename button. You can use the up and down arrows to move a favorite link up or down in the list.
Add Customized Favorite Link	Enter a link name in the Link Name field. The maximum number of characters is 25. You can also enter a link URL address. Be sure to click the Add Favorite Link button when you are done.
Workspace Settings	You can use any of the links as your default Home page by selecting the link from the drop-down menu. To change the number of links allowed on your My Favorites list, select a number from the drop-down menu. The default is 10. (**Note**: This option is not available until you add a shortcut.)

My Preference Page Fields

To edit current your NA Home page preferences, on the NA Home page under My Settings click My Preferences. The My Preference page opens. This page enables you to customize the Home page and specify the Cisco software images that are displayed on the Device Software Image Recommendation page. Refer to "Device Software Image Recommendation Page Fields" on page 225 for information.

Field	**Description/Action**
Show My Tasks and Approval Requests (when Workflow is enabled) on the home page	Select Yes (the default) or No.
Show Recent Changes on the home page	Select Yes (the default) or No.
Show Recent Events on the home page	Select Yes (the default) or No.
Show System Reports on the home page	Select Yes or No (the default).
Show My Favorite Reports on the home page	Select Yes (the default) or No.
Show My Device Groups on the home page	Select Yes (the default) or No.
Software Image Recommendation Settings	
Include only images with a higher version than the current version	Select Yes or No (the default).
Include only images with the same subset feature	Select Yes or No (the default).
Include only general deployment images	Select Yes or No (the default).
Include only latest maintenance release images	Select Yes or No (the default).
Include Cisco.com images for image recommendation	Select Yes (the default) or No.

Be sure to click the Save button when you are finished.

My Permissions Page Fields

The View Permissions page displays the permissions you have due to the groups to which you belong. Keep in mind that there are also assigned roles. Refer to "New User Role Page Fields" on page 261 for information.

Note: If you are not using View Permissions, new users are placed in the View All Partitions group, giving them View Permission to all devices. If you create View Permissions, new users are not implicitly granted any View Permissions.

To view your current permissions, on the NA Home page under My Settings click My Permissions. The My Permissions page opens.

Field	Description/Action
User Groups and Roles	Displays all of the groups you belong to and the roles assigned to each group. Refer to "Adding User Roles" on page 259 for information.
Command Permissions Granted	Displays the permissions you have relative to commands. Refer to "Granting Command Permissions" on page 719 for information.
Modify Device Permissions Granted	Displays the permissions you have to modify devices.
Script Permissions Granted	Displays the permissions you have to run and modify scripts.
View Partitions Permissions Granted	Displays the permissions you have to view users and/or devices. Refer to "Segmenting Devices and Users" on page 150 for information.

Change Password Page Fields

To change your local authentication password and/or your external resource credentials, on the NA Home page under My Settings click Change Password. The Change Password page opens.

Field	Description/Action
Local Authentication Password	
New Password	Enter a new password.
Confirm New Password	Enter the new password again for confirmation and click the Submit button.
External Resource Credentials/Add new external resource credentials	
Credential Type	Select a credential type from the drop-down menu. Options include: • Cisco.com Credentials — This credential is used by Cisco.com for software image recommendations and downloading software images to Cisco devices. Cisco.com contains released versions of system software and drivers for Cisco's internetworking products. Refer to "Download Image From Cisco.com Task Page" on page 369 for information. • Proxy Credentials — This credential is used when access to Cisco.com is through a proxy that requires a username and password.
Username	Enter your username. Keep in mind that the proxy is generic and not directly tied to the Cisco.com. Refer to "Server Page Fields" on page 54 for information on configuring the Software Image Management Collector HTTP Proxy server.
Password	Enter your password.
Confirm Password	Enter your password again for confirmation and click the Add button.

To modify or delete existing external resource credentials, use the Modify and Delete buttons.

What is Quick Launch?

In previous versions of NA, when executing tasks, such as taking a snapshot, checking for policy compliance, or generating reports, you had to navigate away from the current page.

You can customize tasks and quickly launch them with pre-filled data without having to navigate away from the current page. For example, if you are currently viewing the Device Details page for a device and have configured Quick Launch actions, such as taking a snapshot, you can simply click the Quick Launch action displayed under Quick Launches in the "My Workspace" area and the task is automatically run.

Note: Only users with Admin permissions can create, execute, and delete quick launches.

How Do I Configure Quick Launches?

Quick Launch utilizes Task Templates. Task Templates enable you to save task definitions so that you can quickly configure and run new and existing tasks without having to start from scratch.

To add a task to Quick Launch:

1. On the main menu bar under Tasks, click Task Templates. The Task Templates page opens. You can also search for Tasks Templates. Refer to "Searching for Tasks" on page 504 for information.
2. Click the "Add to Quick Launches" link in the Actions column. The Quick Launch link is automatically displayed in the Quick Launches section under the "My Workspace" area. The Quick Launch link assumes the name of the current Task Template. If you want to rename the link, use the displayed pop-up box. Note that the pop-up box is only displayed when there is a duplicate name.

Refer to "Task Templates" on page 282 for detailed information on Task Templates.

If you have not already defined a Task Template, do the following:

1. On the main menu bar under Tasks, select New Tasks and click a task, such as Take Snapshot. The Take Snapshot page opens.
2. On any new or edit task page, click the "Save as Task Template" option in the Save Options field. When you save the task, the task is saved as a template and displayed on the Task Template page.

Managing Quick Launches

To manage Quick Launches, on the NA Home page click the Quick Launch link under My Settings in the "My Workspace" area. The Quick Launch page opens. On this page, you can:

- Adjust the order of the displayed Quick Launches using the arrow buttons or the drag and drop function
- Delete Quick Launches
- Rename Quick Launches
- Determines the size of the Quick Launch area on the NA Home page under the "My Workspace" area.

Refer to "Sample Quick Launch Display" on page 269 for a typical display.

Using Quick Launch

After you have defined Quick Launches, the list of Quick Launches is displayed under the My Settings section in the "My Workspace" area of the NA Home page.

The Quick Launch links depend on the specific page and content where you are working. For example, on the Inventory page, select a device for which you want details. The Device Details page opens for that device. If you have configured a Take Snapshot Quick Launch, click the Take Snapshot link in the Quick Launches section under My Settings in the "My Workspace" area of the NA Home page and the task is automatically run. An information message is displayed, for example `successfully saved task`.

When configuring tasks for Quick Launch, keep in mind that Quick Launches always run against the current device or device group (or Inventory if neither exist). When you configure a task template, you provide the device and/or device group information for the task. This information is replaced with the current device or device group information for the Quick Launch you are running.

For example, if you have configured a Reboot Device Task Quick Launch and then run that Quick Launch on the device for which you are currently viewing, the device is automatically rebooted, regardless of the device and/or device group information your provided on the original task template. You are not prompted before the reboot.

Sample Quick Launch Display

The following table describes the fields in a sample Quick Launch page. Refer to "What is Quick Launch?" on page 267 for information on how to configure Quick Launches.

Field	Description/Action
task templates listing page link	Clicking the link opens the Task Templates page. Refer to "Task Templates" on page 282 for information.
Quick Launch Actions -- Device	
Task name, for example Take Snapshot	The Up and Down arrows enable you to sort the listed Quick Launch device actions.
	The red X icon enables you to delete Quick Launch device actions.
	If you want to change the Quick Launch device action name, enter a new name and click the Rename button. The action name cannot exceed 25 characters.
Quick Launch Actions -- Policy	
Task name, for example Check Policy	The Up and Down arrows enable you to sort the listed Quick Launch policy actions.
	The red X icon enables you to delete Quick Launch device actions.
	If you want to change the Quick Launch policy action name, enter a new name and click the Rename button. The action name cannot exceed 25 characters.

Field	Description/Action
Quick Launch Actions -- Report	
Task name, for example Generate Summary Reports	The Up and Down arrows enable you to sort the listed Quick Launch report actions.
	The red X icon enables you to delete Quick Launch report actions.
	If you want to change the Quick Launch report action name, enter a new name and click the Rename button. The action name cannot exceed 25 characters.
Quick Launch Settings	
Maximum links allowed on Quick Launch	Select a value from the pull-down menu. The default value is 10. This value determines the size of the Quick Launch area on the NA Home page under the "My Workspace" area. Refer to "Editing User Settings" on page 262 for information on the NA Home page.

Customizing the NA Home Page

The NA Home page opens whenever you login to NA. You can also return to the NA Home page by clicking the Home link in the upper left-hand corner of each page.

The NA Home Page includes two frames. The left-hand frame includes:

- Search — The Search options enable you to find devices by Hostname or IP address and connect to them via Telnet or SSH. Refer to “Search/Connect Function” on page 275 for detailed information.
- My Workspace — The My Workspace area includes the following sections:
  - Current Device/Current Device Group (Inventory is the default)
  - My Favorites
  - Quick Launches (if applicable)
  - My Settings

Refer to “Editing User Settings” on page 262 for detailed information on configuring the options in the My Workspace area.

The right-hand frame can be customized to include:

- Workflow approvals
- List of tasks
- Recent configuration changes (what device changed and when)
- Recent system events (such as device access failures)
- Selected device groups
- Selected favorite reports
- Selected system reports

Refer to “My Homepage Tab Fields” on page 272 and “Statistics Dashboard Tab Fields” on page 274 for information.

My Homepage Tab Fields

Field	Description/Action
Workflow Approvals (if applicable)	
Tasks Awaiting My Approval link	Displays the tasks awaiting your approval, including: • Task Name — Displays the task name. If you click the task name, the Task Information page opens, where you can approve the task. Refer to "Task Information Page Fields" on page 678 for information on the Task Information page. • Approve By — Displays the date and time by which the task must be approved. Refer to "Approval Requests" on page 676 for information on task approval. • Approval — Displays the Approval status. • Schedule Date — Displays when the task was scheduled. • Status — Displays the current status. Click the View All link to open the Approval Requests page, where you can view a list of your approval requests. Refer to "Approval Requests" on page 676 for information on the Approval Requests page.
My Tasks	
Task Name	Displays a list of your tasks. Refer to "What Are Tasks?" on page 279 for information. When you first configure NA, a list of default tasks are displayed, including Take Snapshot, Generate Summary Reports, Run Diagnostics, and Data Pruning.
Scheduled Date	Displays the date and time the task was scheduled.
Status	Displays the current task status. For a list of task statuses, refer to "Task Information Page Fields" on page 408.
View All link	Opens the My Tasks page, where you can view all of your tasks. Refer to "What Are Tasks?" on page 279 for information.
Recent Changes	
Time frame	The default time frame is the past 24 hours. You can select the following time frames: • Past 1, 2, 4, 8, 12, 24, and 48 hours • Past 1 and 2 weeks • Past 1 month • All Configs
Date	Displays the date and time of the configuration change.
Device	Displays the host name or IP address of the device that was changed. Clicking the device link opens the Device Details page.
Changed By	Displays the login name of the person who changed the configuration, device, or task. N/A means not applicable.
Comments	Displays any comments about the configuration.

Field	Description/Action
Action	You can select the following actions: • Compare to Previous — Opens the Compare Device Configuration page, where you can view the selected configuration and the next previous configuration side-by-side. The differences are highlighted in different colors to make them easy to view. • View Config — Opens the Device Configuration Detail page, where you can view the entire configuration, deploy this version of the configuration to the device running configuration, edit the configuration, retrieve diagnostics, and compare the configuration to the previous configuration.
View All link	Opens the Configuration Changes page, where you can view all the configuration changes and adjust the time frame in which you view changes. Refer to "Viewing Device Configuration Changes" on page 174 for information.
Recent Events	
Time frame	The default time frame is the past 24 hours. You can select the following time frames: • Past 1, 2, 4, 8, 12, 24, and 48 hours • Past 1 and 2 weeks • Past 1 month • All Configs
Event Summary	Displays the type of event. Click the link to view a complete list of events of this type. Refer to "Consolidated View of Events (SingleView)" on page 552 for information.
Count	Displays the number of events of this type.
Event List Page link	Opens the System & Network Events page, where you can see a longer list of events and adjust the time frame in which you view events. Refer to "Consolidated View of Events (SingleView)" on page 552 for information.
My Device Groups (if applicable)	
Device Group links	Opens the Device Groups page, where you can view the current device groups.
My Favorite Reports (if applicable)	
All Favorite Reports link	Opens the User & System Reports page, where you can view the reports you created from custom searches as well as the System reports.

Statistics Dashboard Tab Fields

The Statistics Dashboard tab provides information on the following:

- Top 5 Vendors
- Top 5 OS Versions
- Top 5 Active Users
- Average Number of Changers Per Day
- Change Frequency
- Top 10 Most Accessed Devices
- Software Level
- OS Inventory
- Configuration Policy Compliance

Refer to "Summary Reports" on page 627 for information.

Search/Connect Function

The NA Home page (and every page) includes a Search Tab on the left-side of each page that enables you to find devices by Hostname or IP address and connect to them via Telnet or SSH. The search function accepts wildcards, so you can quickly find a group of related devices, or at least narrow your search until you find the target device. Refer to "Searching for Devices" on page 474 for information on the Search For Devices page fields.

You can also use the Search For drop-down menu to search for specific:

- Devices
- Interfaces
- Modules
- Policies
- Compliance
- Configurations
- Diagnostics
- Tasks
- Sessions
- Events
- Users
- SingleSearch
- ACLs
- MAC Addresses
- IP Addresses
- VLANs
- Device Templates
- Advanced Search

Chapter 7: Scheduling Tasks

Use the following table to quickly locate information.

Topic	Refer to:
What Are Tasks?	"What Are Tasks?" on page 279
Scheduling Tasks	"Scheduling Tasks" on page 280
Tasks Templates	"Task Templates" on page 282
Configure Syslog Task	"Configure Syslog Task Page Fields" on page 286
Deploy Passwords Task	"Deploy Passwords Task Page Fields" on page 290
Discover Driver Task	"Discover Driver Task Page Fields" on page 295
Reboot Device Task	"Reboot Device Task Page Fields" on page 298
Run ICMP Test Task	"Run ICMP Test Task Page Fields" on page 301
Run Command Script Task	"Run Command Script Task Page Fields" on page 306
Run Diagnostics Task	"Run Diagnostics Task Page Fields" on page 312
Take Snapshot Task	"Take Snapshot Task Page Fields" on page 317
Synchronize Startup and Running Task	"Synchronize Startup and Running Task Page Fields" on page 321
Update Device Software Task	"Update Device Software Task Page Fields" on page 325
Import Devices Task	"Import Devices Task Page Fields" on page 331
Import Users Task	"Import Users Task Page Fields" on page 336
Detect Network Devices Task	"Detect Network Devices Task Page Fields" on page 343
Deduplication Task	"Deduplication Task Page Fields" on page 349
OS Analysis	"OS Analysis Task Page Fields" on page 352
Port Scan	"Port Scan Page Fields" on page 355
Provision Device from Template	"Provision Device Task Page Fields" on page 358
Add Device Context	"Add Device Context Task Page Fields" on page 361
VLAN	"VLAN Task Page Fields" on page 365
Download Image From Cisco.com Task	"Download Image From Cisco.com Task Page" on page 369
Backup Device Software Task	"Backup Device Software Task Page Fields" on page 371

Topic	Refer to:
Check Policy Compliance Task	"Check Policy Compliance Task Page Fields" on page 374
Generate Summary Reports Task	"Generate Summary Reports Task Page Fields" on page 377
Email Report Task	"Email Report Task Page Fields" on page 379
Deploy Remote Agent Task	"Deploy Remote Agent Page Fields" on page 382
Resolve FQDN Task	"Resolve FQDN Task Page Fields" on page 384
Data Pruning Task	"Data Pruning Task Page Fields" on page 387
Run External Application Task	"Run External Application Task Page Fields" on page 390
Scheduling Multi-Task Projects	"Scheduling Multi-Task Projects" on page 393
Viewing My Tasks	"My Tasks Page Fields" on page 399
Viewing Scheduled Tasks	"Viewing Scheduled Tasks" on page 402
Viewing Running Tasks	"Viewing Running Tasks" on page 404
Viewing Recent Tasks	"Viewing Recent Tasks" on page 406
Viewing Task Load	"Viewing Task Load" on page 411

What Are Tasks?

Tasks are the primary mechanism by which HP Network Automation (NA) interacts with your network. Tasks are specific actions you can either schedule or run immediately. The Task Information page provides the results of performed tasks, such as snapshots to identify device and configuration changes and software policy compliance to identify devices that are or are not in compliance.

Running Tasks Against Ad-hoc Device Groups

You can run a task or set of tasks (Multi-Task Project) against a temporary group of devices by creating ad-hoc device groups. You can create ad-hoc device groups by using either:

- The check boxes on the Device List page to select devices and then selecting the task you want to run against the devices using the Actions drop-down menu. Refer to "Viewing Devices" on page 188 for detailed information.
- Importing a CSV file that contains an ad-hoc list of devices. For example, let's say you have 200 devices in your network and there is one DNS server for each group of 50 devices. Instead of creating four device groups (each with 50 servers), you can generate a CSV file that maps the devices to DNS servers. You then can load the CSV file into a command script and run one task to update all of the DNS servers. For information on running command scripts, refer to "Run Command Script Task Page Fields" on page 306.

For information on Multi-Task Projects, refer to "Multi-Task Project Page Fields" on page 395.

Scheduling Tasks

When you create or update a task, you can set a priority for the task so that it runs at higher priority than other tasks. There are five task priority levels, 1 through 5. 1 is the highest task priority level. Higher priority tasks run before lower priority tasks.

All tasks are created with the default task priority level 3. You must have Administrative privileges to set a task to priority level 1, or be granted permission to do so by the NA administrator. Users without this permission can set a task's priority level to between 2 to 5. Refer to “New User Role Page Fields” on page 261 for information on command permissions.

When changing a parent task's priority that is currently running, any existing child tasks that are in the “Pending” or “Waiting” state will appropriately change their priority to that of the parent task. However, child tasks that have not been created yet or are in another state, such as “Running” or “Paused”, will retain the parent task’s original priority. If a parent task is not running and its priority is changed, all of the parent task’s child tasks take on the new priority.

Note: Task-related APIs will have the `-taskpriority` option. For information, see the *NA CLI/API Command Reference*.

Terminology

The following terms are used to describe the NA Task Scheduler.

- **Task** — The smallest unit to be run by the NA Task Scheduler. A task can include one or more child tasks. A task has its own NA Core ID, Task ID, Parent Task ID (optional), priority, and schedule time. For information on NA Core IDs, see the *NA Multimaster Distributed System on Oracle Guide* or the *NA Multimaster Distributed System on SQL Server Guide*.
- **Task Queue** — A group of tasks with the same NA Core ID, Parent Task ID, and priority. If a task does not have Parent Task, its Task ID is used as the Parent Task ID.
- **Task Queue Group** — A group of task queues with the same NA Core ID and priority. There can be a total of five task queue groups.
- **Task Pool** — A total of five task queue groups with the same NA Core ID. The Task Pool is cached in memory and used for task scheduling. It is synchronized with the tasks defined in the database. When you create, update, or delete tasks in the database, NA updates the Task Pool. If the task is for local NA Core, the local Task Pool is updated. If the task is for a remote NA Core, the Task Pool on the remote NA Core is updated.
- **Task Pool Caching** — The Task Pool caches all tasks which have not run yet.

When polling a task out of the Task Pool, NA processes:

1. Task queue groups in the ascending order of their priorities.
2. Tasks in each task queue use the First In, First Out algorithm based on their scheduled time. NA will increase a task's priority if it has been behind schedule for a certain amount of time. All sub-tasks of this task use the new priority. If the task is a recurring task, the new priority will only apply to this task and its sub-tasks in the current occurrence.

Keep in mind that NA will not attempt to run Max Concurrent Tasks if there is not sufficient memory available. As a result, if Max Concurrent Tasks is set to 200, NA might not be able to run all 200 concurrent tasks. Refer to "Server Page Fields" on page 54 for information on setting the maximum number of concurrent tasks.

Note: If a task needs to be rescheduled (schedule time and task priority) by the scheduler (not a user), the new information will only be updated in the Task Pool. It will not be saved in the database nor be available to the user.

Round-robin Group Tasks

When a task completes, NA alternates between taking the next sub-task from Group 1 and then from Group 2. For example, if you started a group task for 10,000 devices at 10am and then started a group task for 10 devices at 10:05am, using the Round-robin algorithm, you no longer have to wait for the first task group to complete before the second group task is started.

Task Templates

Task Templates enable you to save task definitions so that you can easily configure and run new and existing tasks without having to start from scratch. You can also create links to your most often run tasks in the My Favorites section under the "My Workspace" area on the NA Home page.

There are three ways to create a Task Template:

- On any new or edit task page, click the "Save as Task Template" option in the Save Options field. As a result, the task is saved as a template and displayed on the Task Template page. Refer to "NA Tasks" on page 284 for information on configuring tasks.
- Click the Create Template link in the Actions column on the Scheduled Tasks page. Refer to "Scheduled Tasks Page Fields" on page 402 for information.
- Click the Create Template link in the Actions column on the Recent Tasks page. Refer to "Recent Tasks Page Fields" on page 406 for information.

When scheduling a Multi-Task Project and saving the project as a Task Template, you must select all of the devices and/or device groups to which the project applies, due to the project's sub-tasks. You also must have the proper permissions to run Multi-Task Projects. Refer to "Scheduling Multi-Task Projects" on page 393 for information.

Note: You can search for Task Templates on the Search for Tasks page. Refer to "Searching for Tasks" on page 504 for information.

To view your current Task Templates, on the main menu bar under Tasks, click Task Templates. The Task Templates page opens.

Note: You can also navigate to the Task Templates page from the Scheduled Tasks, Running Tasks, and Recent Tasks pages.

Field	Description/Action
My Tasks link	Opens the My Task page. Refer to "My Tasks Page Fields" on page 399 for information.
My Drafts link	Opens the My Drafts page. Refer to "My Tasks Page Fields" on page 399 for information.
Approval Requests link	Opens the Approval Requests page, where you can view tasks needing approval by the currently logged in user. Refer to "Approval Requests" on page 676 for information.
Scheduled Task link	Opens the Scheduled Task page. Refer to "Scheduled Tasks Page Fields" on page 402 for information.
Running Tasks link	Opens the Running Tasks page. Refer to "Running Tasks Page Fields" on page 404 for information.
Recent Tasks	Opens the Recent Tasks page. Refer to "Recent Tasks Page Fields" on page 406 for information.
Check Boxes	You can use the left-side check boxes to delete templates. Once you have selected the template, click the Actions drop-down menu and click Delete. The adjacent Select drop-down menu enables you to select or deselect all templates.

Field	Description/Action
Create Date	Displays the date and time NA began running the task.
Template Name	Displays the template name.
Host/Group	Displays the host or group name of the network device(s) associated with the task. You can click the link to open the Device Information page, where you can view detailed information about the devices in the group.
Priority	Displays the task's priority. There are five task priority levels, 1 through 5. 1 is the highest task priority level. Refer to "Scheduling Tasks" on page 280 for more information.
Partition	If you have created Partitions for security or business reasons, the Partitions are displayed in the column. Refer to "Segmenting Devices and Users" on page 150 for detailed information on creating Partitions.
Created By	Displays the login name of the person who scheduled the task (or the last user to modify the task).
Comments	Displays comments about the task.
Actions	You can select the following actions: • Delete — Opens a dialogue box to confirm that you want to delete the template. Note that when you delete a template, its corresponding favorite link is removed as well. • Edit — Open the Edit Task page for the selected task, for example the Edit Task - Snapshot page. You can then edit the task and save it as a template. (**Note**: Unless you change the name of the template, the new template overrides the old template.) • Run — Opens the Rerun Task page, where you can re- run the task, or edit the task and the run it again. (**Note**: This option only appears if the task can be rerun as configured in the task's "Scheduling Options" field.) • Add to Favorites — Adds the task to the "My Favorites" section in the My Workspace area of the NA Home page so that you can run the task without having to navigate to the task page. • Add to Quick Launches — Adds the Quick Launch link to the Quick Launches section under the "My Workspace" tab on the NA Home page. The Quick Launch link assumes the name of the current Task Template. If you want to rename the link, use the displayed pop-up box. Refer to "What is Quick Launch?" on page 267 for information on Quick Launches.
Display results in groups of	You can set the number of items to display per page from the drop-down menu. The default is 25.

NA Tasks

To open the New Task/Template page, on the menu bar under Tasks, select Task and click the task you want to schedule. The New Task/Template page opens for that task. The following table lists the tasks from which you can choose.

Task	Refer to…
Configure Syslog	"Configure Syslog Task Page Fields" on page 286
Deploy Passwords	"Deploy Passwords Task Page Fields" on page 290
Discover Driver	"Discover Driver Task Page Fields" on page 295
Reboot Device	"Reboot Device Task Page Fields" on page 298
Run ICMP Test	"Run ICMP Test Task Page Fields" on page 301
Run Command Script	"Run Command Script Task Page Fields" on page 306
Run Diagnostics	"Run Diagnostics Task Page Fields" on page 312
Take Snapshot	"Take Snapshot Task Page Fields" on page 317
Sync Startup & Running	"Synchronize Startup and Running Task Page Fields" on page 321
Update Device Software	"Update Device Software Task Page Fields" on page 325
Import Device	"Import Devices Task Page Fields" on page 331
Import User	"Import Users Task Page Fields" on page 336
Detect Network Devices	"Detect Network Devices Task Page Fields" on page 343
Deduplication	"Deduplication Task Page Fields" on page 349
OS Analysis	"OS Analysis Task Page Fields" on page 352
Port Scan	"Port Scan Page Fields" on page 355
Provision Device From Template	"Provision Device Task Page Fields" on page 358
Device Context	"Add Device Context Task Page Fields" on page 361
VLAN	"VLAN Task Page Fields" on page 365
Download Image From Cisco.com Task	"Download Image From Cisco.com Task Page" on page 369
Provision Device From Template	"Provision Device Task Page Fields" on page 358
Download Image From Cisco.com Task	"Download Image From Cisco.com Task Page" on page 369
Backup Device Software Task	"Backup Device Software Task Page Fields" on page 371
Check Policy Compliance	"Check Policy Compliance Task Page Fields" on page 374
Generate Summary Reports	"Generate Summary Reports Task Page Fields" on page 377
Email Report	"Email Report Task Page Fields" on page 379
Deploy Remote Agent	"Deploy Remote Agent Page Fields" on page 382

Task	Refer to…
Resolve FQDN	"Resolve FQDN Task Page Fields" on page 384
Prune Data	"Data Pruning Task Page Fields" on page 387
Run External Application	"Run External Application Task Page Fields" on page 390

Configure Syslog Task Page Fields

The Configure Syslog task enables you to schedule the automatic configuration of one or more devices to send Syslog messages. NA uses Syslog messages to help detect real-time configuration changes.

After discovery (or when you assign a driver to each device), NA:

1. Takes a snapshot of the configuration.
2. Updates the configuration to send Syslog messages to NA.
3. Writes a comment in the configuration indicating that the device was auto-configured to enable change detection.
4. Takes a final snapshot.

Field	Description/Action
Task Name	Displays Configure Syslog. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Applies to	Select one of the following options: • Device / Group — Enter an IP Address, Hostname, or Device Group name on which to run the task against or click the magnifying glass icon. For information on how to use the Device Selector, refer to "Device Selector" on page 144. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Enter comments about the task.

Field	Description/Action
Task Options	
Session Log	To store the complete device session log, click the "Store complete device session log" check box. Keep in mind that all tasks that interact with a device can be run with session logging enabled. This provides a detailed log of the interaction with the device during the task. Session logs should be viewed as the first step to debugging device-specific issue. Session logs provide details on CLI, SNMP, and all transfer protocol actions taken during the task. (**Note**: Large amounts of data could be stored. Refer to "Logging" on page 98 for detailed information on logging.)
Force Save	The device configuration update setting. This setting applies to only those devices that support a startup configuration. The default value of this setting is configurable per task type. • If NA should overwrite the startup configuration with the current running configuration at the completion of this task, select the Force Save check box. • If NA should not change the startup configuration, clear the Force Save check box. (**Note**: This setting is new in NA 9.20. It overrides all other approaches to determining whether to update the device startup configuration.)
Syslog Configuration	Select one of the following options: • Set Device to Log to the NA Syslog Server (the default). • Device Logs to a Syslog Relay, Set the Correct Logging Level. — Enter a Relay Host.
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.
Device Credentials Options Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Device Access page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to "Device Access Page Fields" on page 47 for information on enabling Device Credentials.)	
Device Credentials	Depending on the Device Credentials options enabled on the Server page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use specific task credentials. You are prompted to enter a Username, Password, Confirm Password, Confirm Enable Password, SNMP Read-Only Community String, and a SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)

Field	Description/Action
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.

Field	Description/Action
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the "Store log output generated by this task" checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to "Logging" on page 98 for detailed information on logging.

Be sure to click Save when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status. Refer to "Task Information Page Fields" on page 408 for more information.

If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 399 for more information.

Deploy Passwords Task Page Fields

The Deploy Passwords task enables you change the password settings and SNMP community strings for multiple devices from a central location.

Note: When you deploy a password to a single device that uses network-wide password rules, NA sets the device to use device-specific password information. You can change this setting on the Edit Device page. To deploy a password to a single device, select the Deploy Password option from the Provision menu. Refer to "Provision Menu Options" on page 241.

Keep in mind that if your network uses AAA with NA, you should change passwords through your AAA server, not through NA. Otherwise, NA might lose contact with the devices. In addition, NA does not actually manage AAA passwords, nor does NA manage device-maintained user accounts. NA only manages what is prompted for when you schedule a password deploy for a single device, or the output of the "what this means" links if you schedule a group password deploy.

NA supports password and community string changes for most devices, including menu-driven devices such as the Nortel Baystack 450. Refer to the Driver Release Service (DRS) documentation for detailed information on supported devices. The DRS is an automated driver release and delivery system.

Upon a successful change, NA performs a device snapshot and downloads the changed configuration. To quickly view all recent password or SNMP community string changes, navigate to the Configuration Changes page. Refer to "Viewing Device Configuration Changes" on page 174 for information.

If you use AAA and attempt to change the device password with the password deployment functionality, NA might attempt to connect to the device using the new password, not AAA. However, the device could still expect an AAA login. If necessary, you would have to manually reconfigure the device to use AAA (in case that changed), and reconfigure NA to login to the device using the correct AAA credentials.

Note: In some cases, the Deploy Passwords task might not assign the username portion of the new credentials as part of the required credentials for NA to access a device. This can be seen when you run a Deploy Passwords task making password changes to a device where a username is required to login to the device. When the task completes and a snapshot executes, the error message reports Missing Username. If this occurs, after running the Deploy Passwords task, edit the device and add the username to the "Use device-specific password information" section. Refer to "Device Password Rules Page Fields" on page 134 for information.

Field	Description/Action
Task Name	Displays Deploy Passwords. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Applies to	Select one of the following options: • Device / Group — Enter an IP Address, Hostname, or Device Group name on which to run the task against or click the magnifying glass icon. For information on how to use the Device Selector, refer to "Device Selector" on page 144. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Enter comments about the task.
Task Options	
Session Log	To store the complete device session log, click the "Store complete device session log" check box. Keep in mind that all tasks that interact with a device can be run with session logging enabled. This provides a detailed log of the interaction with the device during the task. Session logs should be viewed as the first step to debugging device-specific issue. Session logs provide details on CLI, SNMP, and all transfer protocol actions taken during the task. (**Note**: Large amounts of data could be stored. Refer to "Logging" on page 98 for detailed information on logging.)

Field	Description/Action
Force Save	The device configuration update setting. This setting applies to only those devices that support a startup configuration. The default value of this setting is configurable per task type. • If NA should overwrite the startup configuration with the current running configuration at the completion of this task, select the Force Save check box. • If NA should not change the startup configuration, clear the Force Save check box. (**Note**: This setting is new in NA 9.20. It overrides all other approaches to determining whether to update the device startup configuration.)
Limited Access Username	Enter the limited access username that NA needs to access the device. Keep in mind that usernames vary depending on the device's vendor and operating system. Click k the "What this means" link for device-specific information. (**Note**: A blank username means that the associated field will not be changed on the device.)
Limited Access Password	Enter the limited access password that NA needs to access the device. Keep in mind that passwords vary depending on the device's vendor and operating system. Click the "What this means" link for device-specific information. (**Note**: A blank password means that the associated field will not be changed on the device.)
Confirm Password	Enter the password again to confirm it.
Full Access Username	Enter the full access username that NA needs to access the device. Keep in mind that usernames vary depending on the device's vendor and operating system. Click the "What this means" link for device-specific information. (**Note**: A blank username means that the associated field will not be changed on the device.)
Full Access Password	Enter the full access password that NA needs to access the device. Keep in mind that passwords vary depending on the device's vendor and operating system. Click the "What this means" link for device-specific information. (**Note**: A blank password means that the associated field will not be changed on the device.)
Confirm Password	Enter the password again to confirm it.
SNMP Read Community Strings	To add an SNMP Read Community String, enter the string in the right-hand box, then click << Add Read Community String. To remove an SNMP Read Community String, select the name in the left-hand box, then click Delete Read Community String. Select "Append to existing community strings on device" (the default) or "Replace existing community strings on device."
SNMP Write Community Strings	To add an SNMP Write Community String, enter the string in the right-hand box, then click << Add Write Community String. To remove an SNMP Write Community String, select the name in the left-hand box, then click Delete Write Community String. Select "Append to existing community strings on device" (the default) or "Replace existing community strings on device."
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.

Field	Description/Action
Device Credentials Options Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Device Access page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to “Device Access Page Fields” on page 47 for information on enabling Device Credentials.)	
Device Credentials	Depending on the Device Credentials options enabled on the Server page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use specific task credentials. You are prompted to enter a Username, Password, Confirm Password, Confirm Enable Password, SNMP Read-Only Community String, and a SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	Not Available

Field	Description/Action
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to “Logging” on page 98 for detailed information on logging.

Be sure to click Save when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task’s start date, duration, and status. Refer to “Task Information Page Fields” on page 408 for more information.

If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to “My Tasks Page Fields” on page 399 for more information.

Discover Driver Task Page Fields

The Discover Driver task enables you to schedule driver discovery.

Field	Description/Action
Task Name	Displays Discover Driver. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Applies to	Select one of the following options: • Device / Group — Enter an IP Address, Hostname, or Device Group name on which to run the task against or click the magnifying glass icon. For information on how to use the Device Selector, refer to "Device Selector" on page 144. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Enter comments about the task.
Task Options	
Session Log	To store the complete device session log, click the "Store complete device session log" check box. Keep in mind that all tasks that interact with a device can be run with session logging enabled. This provides a detailed log of the interaction with the device during the task. Session logs should be viewed as the first step to debugging device-specific issue. Session logs provide details on CLI, SNMP, and all transfer protocol actions taken during the task. (**Note**: Large amounts of data could be stored. Refer to "Logging" on page 98 for detailed information on logging.)
Options	If there is no driver set, check the "Only if No Driver is set" check box (the default).
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.

Field	Description/Action
Device Credentials Options Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Device Access page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to "Device Access Page Fields" on page 47 for information on enabling Device Credentials.)	
Device Credentials	Depending on the Device Credentials options enabled on the Server page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use specific task credentials. You are prompted to enter a Username, Password, Confirm Password, Confirm Enable Password, SNMP Read-Only Community String, and a SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.

Field	Description/Action
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to “Logging” on page 98 for detailed information on logging.

Be sure to click Save when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task’s start date, duration, and status.

Refer to “Task Information Page Fields” on page 408 for more information. If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to “My Tasks Page Fields” on page 399 for more information.

Reboot Device Task Page Fields

The Reboot Device task enables you to reboot devices.

Field	Description/Action
Task Name	Displays Reboot Device. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to “Task Templates” on page 282 for information on Task Templates.
Applies to	Select one of the following options: • Device / Group — Enter an IP Address, Hostname, or Device Group name on which to run the task against or click the magnifying glass icon. For information on how to use the Device Selector, refer to “Device Selector” on page 144. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to “Scheduling Tasks” on page 280 for information on task scheduling.
Comments	Enter comments about the task.
Task Options	
Session Log	To store the complete device session log, click the “Store complete device session log” check box. Keep in mind that large amounts of data could be stored. This option is recommended for device troubleshooting only. Refer to “Logging” on page 98 for detailed information on logging.
Force Save	The device configuration update setting. This setting applies to only those devices that support a startup configuration. The default value of this setting is configurable per task type. • If NA should overwrite the startup configuration with the current running configuration at the completion of this task, select the Force Save check box. • If NA should not change the startup configuration, clear the Force Save check box. (**Note**: This setting is new in NA 9.20. It overrides all other approaches to determining whether to update the device startup configuration.)

Field	Description/Action
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.

Device Credentials Options

Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Device Access page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to "Device Access Page Fields" on page 47 for information on enabling Device Credentials.)

Device Credentials	Depending on the Device Credentials options enabled on the Server page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use specific task credentials. You are prompted to enter a Username, Password, Confirm Password, Confirm Enable Password, SNMP Read-Only Community String, and a SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)

Approval Options

Approval options are only displayed if the task is part of a Workflow Approval Rule.

Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.

Scheduling Options

Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	Not available.

Field	Description/Action
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to “Logging” on page 98 for detailed information on logging.

Be sure to click Save when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task’s start date, duration, and status. Refer to “Task Information Page Fields” on page 408 for more information.

If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to “My Tasks Page Fields” on page 399 for more information.

Run ICMP Test Task Page Fields

The Run ICMP (Internet Control Message Protocol) Test task enables you to schedule either a ping or traceroute test from a device to one or more devices.

Traceroute attempts to trace the path a packet takes through the network. Traceroute transmits packets with small Time-To-Live (TTL) values. TTL is an IP header field that is designed to prevent packets from running in loops, also known as *hop-limit*. Traceroute depends on devices sending an ICMP Time Exceeded message back to the sender. Traceroute causes devices along a packet's normal delivery path to generate these ICMP messages that identify the path.

Packet INternet Groper (Ping) sends a single packet and listens for a single packet in reply. Ping is implemented using the required ICMP Echo function.

In general, the traceroute option performs its action by going from one device to the next along routes that the device knows about. Alternatively, ping goes to each device along the route individually.

Keep in mind that the traceroute and ping commands are not functions that NA completes. The devices do these. NA must be able to login to the source device and then issue the appropriate command for that device to trace to the destination devices. Each device could implement the functionality differently (or not at all). What you see in the ICMP Test Results page is a dump of what the device displays on the screen.

Both ping and traceroute are excellent networking troubleshooting tools. For example, with ping you can test 100 devices to see if they can access a specific device. Or if you see that 20 devices are having a problem accessing a specific device, you can run an automated remote traceroute and check the path each device is taking to that destination.

Note: Use ICMP tests only to verify connectivity occasionally or after a change. They are not a replacement for monitoring software. You should schedule ICMP tests no more than once per 10 minutes.

Field	Description/Action
Task Name	Displays Run ICMP Test. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Applies to	Select one of the following options: • Device / Group — Enter an IP Address, Hostname, or Device Group name on which to run the task against or click the magnifying glass icon. For information on how to use the Device Selector, refer to "Device Selector" on page 144. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Enter comments about the task.
Task Options	
Session Log	To store the complete device session log, click the "Store complete device session log" check box. Keep in mind that all tasks that interact with a device can be run with session logging enabled. This provides a detailed log of the interaction with the device during the task. Session logs should be viewed as the first step to debugging device-specific issue. Session logs provide details on CLI, SNMP, and all transfer protocol actions taken during the task. (**Note**: Large amounts of data could be stored. Refer to "Logging" on page 98 for detailed information on logging.)
Test Type	Select either ping or traceroute.
Target Host List	To add a host, enter the name in the right-hand box, then click << Add Host. To remove a host, select the host name in the left-hand box, then click Remove Host.
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.

Field	Description/Action
Device Credentials Options Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Device Access page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to “Device Access Page Fields” on page 47 for information on enabling Device Credentials.)	
Device Credentials	Depending on the Device Credentials options enabled on the Server page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use specific task credentials. You are prompted to enter a Username, Password, Confirm Password, Confirm Enable Password, SNMP Read-Only Community String, and a SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.

Field	Description/Action
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to “Logging” on page 98 for detailed information on logging.

Be sure to click Save when you are finished. The ICMP Test Result page opens if the task is scheduled to run immediately.

Note: What you see in the ICMP Test Results page is a dump of what the device displays on the screen.

If the task is successful and you selected the ping option, the following information is displayed, depending on the device and the information you entered on the Run ICMP Test Task page:

- Create Date
- Command Run
- Result
- Command Output (for example: `Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms`)

If you selected the traceroute option, the following information is displayed, depending on the device and the information you entered on the Run ICMP Test Task page:

- Create Date
- Command Run
- Result
- Command Output (for example:

  ```
  1 1ms 1ms 1ms 10.255.111.2
  2 4ms 4ms 4ms 10.255.111.3
  3  *   *   *   *
  ```

  The first column displays the hop. The next three columns show the time it took for the device to respond. If the time the device takes to respond is longer than the designated time-out value, asterisks are displayed.). The last column is the host that responded.

If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to “My Tasks Page Fields” on page 399 for information.

Run Command Script Task Page Fields

The Run Command Script task enables you to run command scripts.

Field	Description/Action
New Command Script link	Opens the New Command Script page. Refer to "New Command Script Page Fields" on page 584 for information on writing scripts.
Command Scripts link	Opens the Command Scripts page. Refer to "Command Scripts Page Fields" on page 579 for information.
Task Name	Displays the Run Command Script name. You can enter a different task name, if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Applies to	Select one of the following options: • Device / Group — Enter an IP Address, Hostname, or Device Group name on which to run the task against or click the magnifying glass icon. For information on how to use the Device Selector, refer to "Device Selector" on page 144. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Enter comments about the task.
Task Options	
Session Log	To store the complete device session log, click the "Store complete device session log" check box. Keep in mind that large amounts of data could be stored. Refer to "Logging" on page 98 for detailed information on logging.

Field	Description/Action
Force Save	The device configuration update setting. This setting applies to only those devices that support a startup configuration. The default value of this setting is configurable per task type. • If NA should overwrite the startup configuration with the current running configuration at the completion of this task, select the Force Save check box. • If NA should not change the startup configuration, clear the Force Save check box. (**Note**: This setting is new in NA 9.20. It overrides all other approaches to determining whether to update the device startup configuration.)
Command Script to Run	Select the command script to run. The options will change depending on the type of script you select. Standard command scripts include: • Cisco IOS Initial Setup • Cisco IOS Insert Line into ACL by ACL id • Cisco IOS Insert Line into ACL by Handle • Cisco IOS Remove Line from ACL by ACL id • Cisco IOS Remove Line from ACL by Handle • Compress Flash • Contivity 1100 Deploy SNMP Community Strings • Extended Ping • Full Duplex • ios_7k_reboot • ios_generic_reboot • ios_l3switch_reboot • Passport 8xxx - Deploy Community Strings • Passport 8xxx - Deploy SNMP-v3 Community Strings • Passport 8xxx - Deploy User Passwords • Passport 8xxx - Enable Radius • Passport 8xxx - Enable Web Server • Sample - Provision FastEther Interface • Set Banner • Set Banner Only If Needed • Set Location • Set NTP Server • Turn off directed broadcast • Update Interface
Preview option	Enables you to build the complete script, but not run it. As a result, you can view which commands will run without actually executing the commands.

Field	Description/Action
Limit to script types	Select all (the default) or select one of the following: • ACL Advanced Script • ACL Application Script • ACL Creation Script • ACL Edit Script
Depending on the command script you select, the following options could be displayed.	
Mode	Displays the device access mode, such as Cisco Exec or Nortel Manager. This is similar to the device platform.
Variables	If the script has variable fields to fill in, enter the values. When finished, you can click Update Scripts to view the script that will run with these variable values. Refer to "New Command Script Page Fields" on page 584 for information on defining custom variables.
Device Family	(Advanced Scripting) Displays the name of the device family on which this script runs. A device family is a collection of devices that share a similar configuration CLI command syntax.
Parameters	Enter the parameters for the script.
Script	Displays the device-specific commands to run. You can edit this instance of the script, however your changes are not saved after this instance runs. If there are multiple modes, one instance of the script appears for each mode. **Note:** The height and width of the Script box is controlled by settings in the Administrative Settings page, User Interface tab. If you use the scripting feature extensively, you may want to adjust these settings so that you can see the script without scrolling.
Deploy option	To run scripts line-by-line rather than deploying in bulk, check the "Run scripts line-by-line..." check box. Keep in mind that devices that are able to run scripts through a bulk deployment method (such as Cisco IOS configuration scripts) do so whenever possible. The default is that the entire contents of the script is deployed and run in a single batch. If an error occurs, the script keeps going. Running a script line-by-line in such cases will result in the script capturing the error and stopping execution.
Wait Option	Checked by default. If you uncheck this option, the task is allowed to run even if there is already another task running against the same device.
Language	(Advanced Scripting) Displays the language in which the script was written.
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.

Field	Description/Action
Device Credentials Options Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Device Access page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to "Device Access Page Fields" on page 47 for information on enabling Device Credentials.)	
Device Credentials	Depending on the Device Credentials options enabled on the Server page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use specific task credentials. You are prompted to enter a Username, Password, Confirm Password, Confirm Enable Password, SNMP Read-Only Community String, and a SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)
Pre-Task / Post-Task Snapshot Options Snapshot options only appear if the system is configured to enable user overrides on the Configuration Mgmt Page under Administrative Settings. (Refer to "Configuration Mgmt Page Fields" on page 38 for information.)	
Pre-Task Snapshot	Select one of the following options: • None (the default) • As part of task
Post-Task Snapshot	Select one of the following options: • None • As part of task (the default) • Scheduled as a separate task
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.

Field	Description/Action
Scheduling Options	
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to “Logging” on page 98 for detailed information on logging.

Be sure to click Save when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status. Refer to "Task Information Page Fields" on page 408 for more information.

If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 399 for more information.

Run Diagnostics Task Page Fields

The Run Diagnostics task enables you to schedule the running of diagnostics. On the menu bar under Tasks, select New Tasks and click Run Diagnostics. The Run Diagnostics page opens.

Field	**Description/Action**
New Diagnostic link	Opens the New Diagnostics page. Refer to "New Diagnostic Page Fields" on page 557 for information.
Diagnostic link	Opens the Diagnostics page. Refer to "Diagnostics Page Fields" on page 555 for information on managing diagnostics.
Task Name	Displays Run Diagnostics. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Applies to	Select one of the following options: • Device / Group — Enter an IP Address, Hostname, or Device Group name on which to run the task against or click the magnifying glass icon. For information on how to use the Device Selector, refer to "Device Selector" on page 144. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Enter comments about the task.
Task Options	
Session Log	To store the complete device session log, click the "Store complete device session log" check box. Keep in mind that large amounts of data could be stored. Refer to "Logging" on page 98 for detailed information on logging.

Field	Description/Action
Force Save	The device configuration update setting. This setting applies to only those devices that support a startup configuration. The default value of this setting is configurable per task type. • If NA should overwrite the startup configuration with the current running configuration at the completion of this task, select the Force Save check box. • If NA should not change the startup configuration, clear the Force Save check box. (**Note**: This setting is new in NA 9.20. It overrides all other approaches to determining whether to update the device startup configuration.)
Diagnostics to Run	Select the diagnostic to run. Use Ctrl+click to select/deselect additional diagnostics. Diagnostics include: • Hardware Information • Memory Troubleshooting • NA Detect Device Boot • NA Device File System • NA Duplex Data Gathering • NA Flash Storage Space • NA Interfaces • NA Module Status • NA OSPF Neighbors • NA Routing Table • NA Topology Gathering • NA VLAN Data Gathering • NA Port Scan **Note**: For detailed information on diagnostics, refer to "View Menu Options" on page 203.
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.

Field	Description/Action
Device Credentials Options Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Device Access page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to "Device Access Page Fields" on page 47 for information on enabling Device Credentials.)	
Device Credentials	Depending on the Device Credentials options enabled on the Server page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use specific task credentials. You are prompted to enter a Username, Password, Confirm Password, Confirm Enable Password, SNMP Read-Only Community String, and a SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)
Pre-Task / Post-Task Snapshot Options Snapshot options only appear if the system is configured to enable user overrides on the Configuration Mgmt Page under Administrative Settings. (Refer to "Configuration Mgmt Page Fields" on page 38 for information.)	
Pre-Task Snapshot	Select one of the following options: • None (the default) • As part of task
Post-Task Snapshot	Select one of the following options: • None • As part of task (the default) • Scheduled as a separate task
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.

Field	Description/Action
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to “Logging” on page 98 for detailed information on logging.

Be sure to click Save when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task’s start date, duration, and status. Refer to “Task Information Page Fields” on page 408 for more information.

If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to “My Tasks Page Fields” on page 399 for more information.

Take Snapshot Task Page Fields

The Take Snapshot task enables you to schedule a snapshot. A snapshot checks whether the stored configuration matches the running configuration on the device. If not, the task stores a new copy of the device configuration and related data in the NA database.

If you select the “Make Snapshot a Checkpoint” option, the NA database is updated even if NA does not detect a difference. As a result, the snapshot still appears as a configuration change on the Home page, Summary reports, Configuration Change search results, and so on.

Field	Description/Action
Task Name	Displays Take Snapshot. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to “Task Templates” on page 282 for information on Task Templates.
Applies to	Select one of the following options: • Device / Group — Enter an IP Address, Hostname, or Device Group name on which to run the task against or click the magnifying glass icon. For information on how to use the Device Selector, refer to “Device Selector” on page 144. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to “Scheduling Tasks” on page 280 for information on task scheduling.
Comments	Enter comments about the task.
Task Options	
Session Log	Check the “Store complete device session log” box to store a debugging log. Keep in mind that all tasks that interact with a device can be run with session logging enabled. This provides a detailed log of the interaction with the device during the task. Session logs should be viewed as the first step to debugging device-specific issue. Session logs provide details on CLI, SNMP, and all transfer protocol actions taken during the task. (**Note**: Large amounts of data could be stored. Refer to “Logging” on page 98 for detailed information on logging.)

Field	Description/Action
Force Save	The device configuration update setting. This setting applies to only those devices that support a startup configuration. The default value of this setting is configurable per task type. • If NA should overwrite the startup configuration with the current running configuration at the completion of this task, select the Force Save check box. • If NA should not change the startup configuration, clear the Force Save check box. (**Note**: This setting is new in NA 9.20. It overrides all other approaches to determining whether to update the device startup configuration.)
Options	Select one or both of the following options: • Make Snapshot a Checkpoint — Copies the running configuration to the NA database rather than checking first whether the stored configuration differs from the running configuration. Note that this option stores the configuration file regardless of whether it changed. However, even if there is no change, the snapshot still appears as a configuration change on the Home page, Summary reports, Configuration Change search results, and so on. As a result, the number of configuration changes includes the check-pointed configurations, and therefore these counts might not be accurate. • Retrieve Binary Configuration — Copies the binary configuration, if any, as well as any text information to the NA database.
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.

Device Credentials Options

Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Device Access page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to “Device Access Page Fields” on page 47 for information on enabling Device Credentials.)

Device Credentials	Depending on the Device Credentials options enabled on the Server page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use specific task credentials. You are prompted to enter a Username, Password, Confirm Password, Confirm Enable Password, SNMP Read-Only Community String, and a SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)

Field	Description/Action
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.

Field	Description/Action
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to “Logging” on page 98 for detailed information on logging.

Be sure to click Save when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task’s start date, duration, and status. Refer to “Task Information Page Fields” on page 408 for more information.

If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to “My Tasks Page Fields” on page 399 for more information.

Synchronize Startup and Running Task Page Fields

The Synchronize Startup and Running task enables you to synchronize the startup and running of configurations for a device. NA will overwrite the startup configuration with the current running configuration. This task ensures that when the device reboots, the current configuration will continue to run.

Field	Description/Action
Task Name	Displays Synchronize Startup and Running. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Applies to	Select one of the following options: • Device / Group — Enter an IP Address, Hostname, or Device Group name on which to run the task against or click the magnifying glass icon. For information on how to use the Device Selector, refer to "Device Selector" on page 144. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Enter comments about the task.
Task Options	
Session Log	Check the "Store complete device session log" box to store a debugging log. This is useful when debugging a failed snapshot, however large amounts of data can be stored. Refer to "Logging" on page 98 for detailed information on logging.

Field	Description/Action
Force Save	The device configuration update setting. This setting applies to only those devices that support a startup configuration. The default value of this setting is configurable per task type. • If NA should overwrite the startup configuration with the current running configuration at the completion of this task, select the Force Save check box. • If NA should not change the startup configuration, clear the Force Save check box. (**Note**: This setting is new in NA 9.20. It overrides all other approaches to determining whether to update the device startup configuration.)
Options	Select the "Bypass if in sync" box if you want NA to skip the task if the configurations are already synchronized.
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.
Device Credentials Options Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Device Access page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to "Device Access Page Fields" on page 47 for information on enabling Device Credentials.)	
Device Credentials	Depending on the Device Credentials options enabled on the Server page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use specific task credentials. You are prompted to enter a Username, Password, Confirm Password, Confirm Enable Password, SNMP Read-Only Community String, and a SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)
Pre-Task / Post-Task Snapshot Options Snapshot options only appear if the system is configured to enable user overrides on the Configuration Mgmt Page under Administrative Settings. (Refer to "Configuration Mgmt Page Fields" on page 38 for information.)	
Post-Task Snapshot	Select one of the following options: • None • As part of task (the default) • Scheduled as a separate task

Field	Description/Action
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.

Field	Description/Action
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to “Logging” on page 98 for detailed information on logging.

Be sure to click Save when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task’s start date, duration, and status. Refer to “Task Information Page Fields” on page 408 for more information.

If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to “My Tasks Page Fields” on page 399 for more information.

Update Device Software Task Page Fields

The Update Device Software task enables you to schedule the deployment of software to one or more devices. Refer to "Software Images" on page 446 for more information. Keep in mind that:

- Total memory is the total physical memory on the device.
- Free memory is the free memory available for uploads at the time of the last memory diagnostic.
- Net memory is the estimate of free memory after the Update Device Software task is run, taking into account any files you marked to be added or removed from the device (but not taking into account the squeeze pre or post processing task).

Field	Description/Action
Task Name	Displays Update Device Software. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Applies to	Select one of the following options: • Device / Group — Enter an IP Address, Hostname, or Device Group name on which to run the task against or click the magnifying glass icon. For information on how to use the Device Selector, refer to "Device Selector" on page 144. • Restrict to devices in partition — Select a partition. Software images will be updated on devices in the specified partition only. Click the More... link for additional information on setting device restrictions. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Enter comments about the task.

Field	Description/Action
Task Options	
Session Log	Check the “Store complete device session log” box to store a debugging log. This is useful when debugging a failed snapshot, however large amounts of data can be stored. Refer to “Logging” on page 98 for detailed information on logging.
Force Save	The device configuration update setting. This setting applies to only those devices that support a startup configuration. The default value of this setting is configurable per task type. • If NA should overwrite the startup configuration with the current running configuration at the completion of this task, select the Force Save check box. • If NA should not change the startup configuration, clear the Force Save check box. (**Note**: This setting is new in NA 9.20. It overrides all other approaches to determining whether to update the device startup configuration.)
Deployment Table	If you are deploying software to a single device, the Deployment Table opens. Refer to “Deployment Table” on page 329 for information.
Image Set	Select the name of the software images you are deploying.
Slot	Select the slot to which you want to deploy the software. NA lists all the slots currently in the NA database.
Memory Preparation	Select one of the following options: • None — Do not prepare the device memory before updating the software. You should manually ensure that the device has enough memory to receive the new software, otherwise the task will fail. • Compact device memory on selected slot — Before deploying software, NA executes a command to compact memory, such as the Cisco IOS squeeze command, if one is supported by the device. No files are removed from the device. You should still ensure that sufficient memory will be available for the update. • Delete files from selected slot, then compact memory — Before deploying software, NA deletes all boot images on the flash (all .bin, .tar, .Z, and .W files), then compacts the memory, if the device supports a compact command. (**Note**: If the deploy software task fails, followed by a device power failure or reboot, the device might not be bootable.)
Verify	If selected, the Verify option verifies images using commands available on the device. The MD5 checksum on the device is compared to the MD5 checksum stored in the database. Keep in mind that if the device does not support this option, the driver will run a Verify command against the image.
Reboot	Check the “Reboot device after deploying software” box to run a script to reboot the device after software deployment. Enter the number of seconds to pause after rebooting before taking a snapshot of the configuration in the “Pause after Reboot” box. The default is 60 seconds.
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.

Field	Description/Action
Device Credentials Options Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Device page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to “Device Access Page Fields” on page 47 for information on enabling Device Credentials.)	
Device Credentials	Depending on the Device Credentials options enabled on the Server page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use specific task credentials. You are prompted to enter a Username, Password, Confirm Password, Confirm Enable Password, SNMP Read-Only Community String, and a SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.

Field	Description/Action
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to “Logging” on page 98 for detailed information on logging.

Deployment Table

The Deployment Table provides advanced options for deploying software to a single device. The data is based on the last File System diagnostic.

Field	Description/Action
Run a File System Diagnostic link	Opens the New Task - Run Diagnostics page, where you can schedule a File System diagnostic to be run on the device. (Refer to "Run Diagnostics Task Page Fields" on page 312 for information.)
Preprocessing tasks	Before deploying software, NA executes a command to compact memory, such as the Cisco IOS squeeze command, if one is supported by the device. No files are removed from the device. You should still ensure that sufficient memory will be available for the update.
File area	The file area contains the following sections: • On Device—Displays the contents of the file systems on the device. For each file system, NA displays the total size, the free space, and the net free space after the device software update. If the net free space is a negative number, the device file system is not large enough for the planned update. • Software Image Repository—Displays the software image sets for the current device that are defined in NA and not currently on the device. For each file, NA displays the file size and, if applicable, a compliance warning. (**Note**: Compliance warnings are not displayed by default. Refer to "User Interface Page Fields" on page 63 for information.) Work with files as follows: • To move a file to the device, drag it from the Software Image Repository to the correct file system. To undo the move, drag the file back to the Software Image Repository. • To remove a file from the device, right-click that file name, and then click **Mark for deletion**. • To set the boot image, right-click the name of a file that is already on or targeted to be on the device, and then click **Mark as boot image**. (**Note**: Only one file can be the boot image. Setting a second file to be the boot image clears the selection of the first file.) • To set the OS image, right-click the name of a file that is already on or targeted to be on the device, and then click **Mark as OS image**. (**Note**: Only one file can be the OS image. Setting a second file to be the OS image clears the selection of the first file.) • To clear the file removal, boot image, or OS image selection, right-click that file name, and then click **Remove marker**.
PostProcessing tasks	After deploying software, NA executes a command to compact memory, such as the Cisco IOS squeeze command, if one is supported by the device. No files are removed from the device. You should still ensure that sufficient memory will be available for the update.
Summary	Displays the changes to be made.
Verify	If selected, the Verify option verifies images using commands available on the device. The MD5 checksum on the device is compared to the MD5 checksum stored in the database. Keep in mind that if the device does not support this option, the driver will run a Verify command against the image.

Field	Description/Action
Reboot	Check the “Reboot device after deploying software” box to run a script to reboot the device after software deployment. Enter the number of seconds to pause after rebooting before taking a snapshot of the configuration in the “Pause after Reboot” box. The default is 60 seconds.

Note: On devices with multiple images installed, NA provides the ability to designate which image should be the Boot image and/or OS image. Please note that this functionality is only available on devices running Cisco IOS.

Be sure to click Save when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task’s start date, duration, and status. Refer to “Task Information Page Fields” on page 408 for more information.

If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to “My Tasks Page Fields” on page 399 for more information.

Note: If the images you have selected to deploy do not fit in the device’s available free disk space, an error message is displayed. You can either return to the task and make changes or deploy the software. It is possible that the disk space calculation is in error.

Import Devices Task Page Fields

The Import Devices task reads data from a comma-separated values (CSV) format file. Each row in the CSV file describes one database object. For device data, the values in the primaryIPAddress and hostName columns, combined with the values in the optional siteName column, uniquely identify the objects. For device group data, the values in the deviceGroupName column uniquely identify the objects. For device-specific passwords, the values in the deviceIPAddress column uniquely identify the objects.

It is recommended that you create network-wide device password rules before importing devices. You can also import a set of device-specific data from one file, and then import the device password data from a second file.

For each row in the CSV file, NA updates the database as follows:

- If the unique identifier does not exist, NA creates a new object using the values specified in the file.
  - Empty cells equate to NULL.
  - NA uses default values for database columns that are not included in the CSV file.
- If the unique identifier exists, NA does the following:
  - If the Overwrite Existing Devices flag is set, NA updates the database object with the values specified in the CSV file. (Empty cells equate to NULL.)

    Note: NA does not modify existing device groups.
  - If the Overwrite Existing Devices flag is not set, NA ignores that row and makes no changes to that database object.

You can import new database objects and modifications to existing database objects from one CSV file. Be sure to completely populate any column included in the CSV file.

Tip: In the CSV file, include only those columns for which you want to set values. If some objects in your data set require columns that do not apply to other objects, create multiple CSV files and multiple import tasks.

To import device data:

1. Create a CSV import file as described in "Creating CSV Files for Importing Device Data" on page 128.

   Note: If the Overwrite Existing Devices option is set to Yes on the Admin > Administrative Settings > Server page, the data in the CSV file overwrite the data in NA. If you do not want certain fields overwritten, remove those fields from the CSV table.

2. Navigate to the New Task/Template - Import Devices page.
3. Make your configuration choices. (See the "Import Device Data Task Page Fields" table on page 332.)
4. Click Save to apply your changes.

Import Device Data Task Page Fields

Field	Description/Action
Device Import Admin Settings link	Opens the Administrative Settings page (Server tab), where you can set NA task limits, enable Workflow, Configure Syslog, and so on.
Task Name	Set the name of this task.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Site	Provides a drop-down menu where you can select a Partition. This field is only displayed if you have configured one or more Partitions. Refer to "Segmenting Devices and Users" on page 150 for information about Partitions. **Note**: This value can be set at device or device group creation only. The value in the siteName column of the CSV file takes precedence over the Site selected here.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Enter comments about the task.
Task Options	
Import File	Enter the name of the CSV file containing the import data. • If the file is on the local system, you can use the Browse button to locate the file. • If the file is on the NA server, include the full path to the file on the NA server.

Import Device Data Task Page Fields (cont'd)

Field	Description/Action
Data Type	Select one of the following options and enter the data you are importing: • Devices — The device CSV template contains all available fields for importing network device data into NA. • Device Group — The device group CSV template contains all available fields for importing device group data into NA. • Passwords — The device passwords CSV template is only required if you are not using device password rules. If you are using a template to create a new CSV file, click the link to open the template file. Save the file to a location on the local system, and then modify the contents to fit your device data, deleting unused columns. For more information, see "Creating CSV Files for Importing Device Data" on page 128.
Syslog Configuration	Select one of the following options: • Set Device to Log to the NA Syslog Server • Device Logs to a Syslog Relay, set the correct logging level • Do not configure syslog Check the "Run Discover Drivers on newly imported Devices" box if you want NA to discover device drivers for the devices associated with the CSV file you are importing. This option requires valid device passwords and community strings. Therefore, you should only use the option when you already have passwords and device password rules set up and debugged for your network or when you import the second file containing device password information. Check the Deactivate inactive or missing devices check box if you want NA to deactivate devices that have not been accessed or imported successfully in the last 45 days.
Preprocess Command	To automate and schedule the entire process within NA, enter the name (and path) of the script file to run before importing the data. This field needs the full executable command which runs in the command/shell console on the server. For example, "perl" needs to be specified if the filter is a PERL script for Windows: `perl c:/filter.pl`
Log filename	Enter the name of the file to which NA will write information about the import task. The log file is helpful when debugging import problems. Check the "Append to log file" if you want NA to append this data to the existing log file. Otherwise, NA will overwrite any existing data in the log file.
Device Origin	Enter the name you want to give this import file. This is useful when you import data on a recurring basis and need to differentiate different data sources and dates.
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.

Import Device Data Task Page Fields (cont'd)

Field	Description/Action
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.

Import Device Data Task Page Fields (cont'd)

Field	Description/Action
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the "Store log output generated by this task" checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to "Logging" on page 98 for detailed information on logging.

Be sure to click Save when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status. Refer to "Task Information Page Fields" on page 408 for more information.

If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 399 for more information.

Import Users Task Page Fields

The Import Users task reads data from a comma-separated values (CSV) format file. Each row in the CSV file describes one database object. For user account data, the values in the userName column uniquely identify the objects. For user group data, the values in the userGroupName column uniquely identify the objects.

For each row in the CSV file, NA updates the database as follows:

- If the unique identifier does not exist, NA creates a new object using the values specified in the file.
  - Empty cells equate to NULL.
  - NA uses default values for database columns that are not included in the CSV file.
- If the unique identifier exists, NA does the following:
  - If the Overwrite Existing User or User Group flag is set, NA updates the database object with the values specified in the CSV file. (Empty cells equate to NULL.)
  - If the Overwrite Existing User or User Group flag is not set, NA ignores that row and makes no changes to that database object.

You can import new database objects and modifications to existing database objects from one CSV file. Be sure to completely populate any column included in the CSV file.

Tip: In the CSV file, include only those columns for which you want to set values. If some objects in your data set require columns that do not apply to other objects, create multiple CSV files and multiple import tasks.

To import user data:

1. Create a CSV import file as described in "Creating CSV Files for Importing User Data" on page 339.

   Note: If the Overwrite Existing User or User Group option is set to Yes on the Admin > Administrative Settings > Server page, the data in the CSV file overwrite the data in the NA database. If you do not want certain fields overwritten, remove those columns from the CSV file.

2. Navigate to the New Task/Template - Import Users page.
3. Make your configuration choices. (See the "Import User Data Task Page Fields" table on page 337.)
4. Click Save to apply your changes.

Import User Data Task Page Fields

Field	Description/Action
User Import Admin Settings link	Opens the Administrative Settings page (Server tab), where you can set NA task limits, enable Workflow, Configure Syslog, and so on.
Task Name	Set the name of this task.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Enter comments about the task.
Task Options	
Import File	Enter the name of the CSV file containing the import data. • If the file is on the local system, you can use the Browse button to locate the file. • If the file is on the NA server, include the full path to the file on the NA server.
Data Type	Select one of the following options and enter the data you are importing: • User — The user CSV template contains all available fields for importing user account data into NA. • User Group — The user group CSV template contains all available fields for user group data into NA. If you are using a template to create a new CSV file, click the link to open the template file. Save the file to a location on the local system, and then modify the contents to fit your user data, deleting unused columns. For more information, see "Creating CSV Files for Importing User Data" on page 339.
Preprocess Command	To automate and schedule the entire process within NA, enter the name (and path) of the script file to run before importing the data. This field needs the full executable command which runs in the command/shell console on the server. For example, "perl" needs to be specified if the filter is a PERL script for Windows: `perl c:/filter.pl`
Log filename	Enter the name of the file to which NA will write information about the import task. The log file is helpful when debugging import problems. Check the "Append to log file" if you want NA to append this data to the existing log file. Otherwise, NA will overwrite any existing data in the log file.

Import User Data Task Page Fields (cont'd)

Field	Description/Action
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.

Import User Data Task Page Fields (cont'd)

Field	Description/Action
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the "Store log output generated by this task" checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to "Logging" on page 98 for detailed information on logging.

Creating CSV Files for Importing User Data

Use the import device data task to import information about user accounts or user groups into NA from CSV files. The first row of the CSV file contains the NA database column names for the data you are importing. Each additional row represents one user account or user group.

NA provides templates for the CSV files. Note the following:

- Do not include columns unless you are populating them. An empty value overwrites existing data if the device already exists.
- The column names must match the database column names. Do not change the database column names set by NA.
- Because the data fields are comma-delimited, fields can include whitespace but not commas (,). Use a colon (:) to separate values within a field.
- Column order is not significant.

To create a CSV file for import:

1. Navigate to the New Task/Template - Import Users page.
2. Under Task Options, Data Type, click the appropriate CSV template link.
3. In an editing tool, do the following:
   - Add information to the data table.
   - To prevent overwriting existing data, delete any unused columns.
   - For information about the columns in the CSV file, see the appropriate section:
     - "User Account Data Import File" on page 340
     - "User Group Import File" on page 341

   Note: For a CSV file containing non-English characters, edit the file in a text editor, not Microsoft Office Excel. Save the CSV file with UTF-8 encoding.
4. Save the file as type CSV on the local system.

User Account Data Import File

The *user.csv* template file contains the NA database column names for user account data. During import, NA uses the values in the userName column to uniquely identify user accounts in the database.

User Account Data Import Fields

Column Name	Description/Action
userName	The user name for logging on to NA, for example Operator or Administrator. This column must be included in each user account data import file. **Note**: User names can contain alphanumeric characters, periods (.), underscores (_), hyphens (-), and backslashes(\) only. **Note**: This value can be set at user creation only.
siteName	The name of the site (partition) to which the user account belongs. The user account will only be visible to other users who have view permission to that partition. **Note**: This value can be set at user creation only.
userGroupName	A colon-separated list of the user groups that contain the user account.
firstName	The first name of the user.
lastName	The last name of the user.
userPassword	The password for the user account. When creating new user accounts, this column must be included.
emailAddress	The email address of the user.
passwordOption	A colon-separated list of the password options for the user account. Specify one or more of the following numeric values: • 1 — User must change password at next logon • 2 — User cannot change password • 4 — Password never expires • 6 — User cannot change password and password never expires • 8 — Account is locked out • 9 — User must change password at next logon and account is locked out • 10 — User cannot change password and account is locked out • 12 — Password never expires and account is locked out • 14 — User cannot change password, password never expires, and account is locked out Refer to “Configuring User Passwords” on page 252 for information on setting password options.
aaaUserName	The AAA (TACACS+ or RADIUS) user name for this user.
aaaPassword	The AAA password for the AAA user name.

User Account Data Import Fields (cont'd)

Column Name	Description/Action
useAaaLoginForProxy	The proxy setting. Specify one of the following numeric values: • 0 — Disabled (use the NA credentials for this user account when authenticating into the telnet/SSH proxy) • 1 — Enabled (use the AAA credentials for this user account when authenticating into the telnet/SSH proxy)
status	The status of the user account. Specify one of the following numeric values: • 0 — Enabled • 1 — Disabled
allowFailover	The authentication failover setting. Specify one of the following numeric values: • 0 — Disabled (prevent user authentication if the external authentication server cannot be reached) • 1 — Enabled (use local authentication if the external authentication server cannot be reached)
userCustom[1-6]	If additional user fields are defined on the Custom Data Setup page, you can import data for any of those fields. Use the column headings as defined in the template file.
comments	Additional information (255 character maximum) about the user account. Do not include commas (,).

User Group Import File

The *user_group.csv* template file contains the NA database column names for user group data. During import, NA uses the values in the userGroupName column to uniquely identify user groups in the database.

Tip: To apply a customized permission role to a user group, do one of the following:

- Create a new user role on the Admin > User Roles & Permissions page, and then specify that role in the CSV file.
- Remove the permissions columns from the CSV file. After importing the new user groups, configure customized permission roles to each new user group in the NA console.

User Group Data Import File Fields

Column Name	Description/Action
userGroupName	The name (255 character maximum) of the user group. This column must be included in each user group data import file.
siteName	The name of the site (partition) to which the user group belongs. **Note**: This value can be set at user group creation only.

User Group Data Import File Fields (cont'd)

Column Name	Description/Action
description	Description text (255 character maximum) about the user group. Do not include commas (,).
commandPermission	The command permission type. Specify one of the following values: • NONE • A colon-separated list of existing command permission roles to assign to the user group.
scriptPermission	The script permission type. Specify one of the following values: • ALL • NONE • A colon-separated list of existing script permission roles to assign to the user group.
viewPermission	The view partition permission type. Specify one of the following values: • ALL • NONE • A colon-separated list of existing view partition permission roles to assign to the user group.
deviceModificationPermission	The modify device permission type. Specify one of the following values: • ALL • NONE • A colon-separated list of existing modify device permission roles to assign to the user group.

Detect Network Devices Task Page Fields

Detecting network devices enables you to locate devices on your network that you want to place under NA management. Once you provide a range of IP addresses, NA scans your network looking for devices. Newly discovered devices are automatically added, along with the appropriate device drivers. In addition, if the Primary IP Address Reassignment option is checked on the Administrative Settings — Server page, NA automatically assigns the correct IP address to a device if the device has multiple IP addresses and interfaces. Consequently, a device is only entered into the system once. Refer to "Device Access Page Fields" on page 47 and "Server Page Fields" on page 54 for task settings.

If you select Driver Discovery on the task page, after NA adds the device to the system, it polls the device to see what type of device it is and subsequently assigns the appropriate device driver to manage the device. NA then takes a snapshot of the device and downloads the configuration and asset information from the device into the database.

For unsupported hosts, a group is also created and added to the system (Inventory). To make sure that unsupported devices are not added as active (and therefore count towards the device's license) and to prevent any operation performed against Inventory that would include these devices, all devices from unsupported hosts are set to inactive by default.

If you want to perform tasks against these devices, you must first activate them. You can activate devices from either the:

- Device Details page, using the Provision menu (Activate Device option).
- Group Device page, where you can select devices using the check boxes and then select the Activate option from the Actions drop-down menu.

When running the Detect Network Devices task, the Task Information page shows:

- Active nodes — Active nodes are IP addresses that responded to either an SNMP scan or an Nmap scan. A node is considered active if it can be managed by NA. Refer to the *HP Network Automation Device Driver Reference* for a list of supported devices.
- Non-active nodes — Non-active nodes are IP addresses that did not respond to either an SNMP scan or an Nmap scan, or both. A device might not respond to an SNMP scan if an incorrect community string is use by NA to query the device.
- Unsupported hosts — Unsupported hosts are IP addresses that responded to either an SNMP scan or an Nmap scan. However in the case of SNMP, it returned a SysOID that NA does not support. In the case of Nmap, the operating system fingerprint returned no matches that NA supports.
- Existing devices — Existing devices indicate that the device's IP address is already known to NA and exists in the system as either the primary IP address of the device or the IP address appears in the database as a result of the BasicIP diagnostic.

Scanning Methods

There are two types of Internet Protocol (IP) traffic:

- User Datagram Protocol (UDP) — UPD is a simple message-based connectionless protocol. With UDP, packets are sent across the network in chunks. In general, UDP is rather unreliable and the order of arriving packets is not guaranteed.
- Transmission Control Protocol (TCP) — TCP is a connection-oriented protocol. TCP is very reliable and the order in which packets are received along a connection is guaranteed.

SNMP scanning uses UDP. SNMP attempts connections to systems using known SYSOIDs to identify network devices. The SNMP scanning method has less impact on your network because it does not require multiple connections to each system. In addition, SNMP is fast, however it can be bogged down if there are a lot of password rules, since all password rules are tried for every IP address scanned. Also, SNMP requires login credentials (community strings) to be successful.

Nmap Scanning uses TCP, although it can be configured to use UDP for some tasks. Because Nmap is a port scanner, if you do not want your network scanned, you should opt for the SNMP scanning method. In addition, Nmap makes many connections to devices so as to test the various ports.

Keep in mind that Nmap does not login to devices, and therefore does not need login credentials. Nmap can range from fast to slow, depending on the network configuration and the IP addresses being scanned. Scanning IP addresses, for example 192.168.0.0, can be very slow. It is highly recommended that you only scan IP address ranges that are within your own organization.

Note: Many organizations have monitoring systems that will send alarms if they detect a network scan in progress. If you are using Nmap to detect network devices, make sure your IT team is fully aware of the scheduled activity.

Defining IP Address Ranges

You must specify at least one IP address inclusion range. You can define ranges two ways:

- CIDR (Classless InterDomain Routing) notation — CIDR denotes a block or range of IP addresses, for example 10.255.1.0/24. This represents an IP address range from 10.255.1.0 to, and including, 10.255.1.255. In total, 256 IP addresses. The /24 in the 10.255.1.0/24 CIDR notation represents how many bits make up the CIDR block's prefix. In this case, it is 24 bits. The balance of the block (the final eight bits) are considered wildcards. Other examples include:
  - 192.168.100.1/32 is a single host 192.168.100.1. (Note all 32 bits make up the prefix without any wildcard bits.)
  - 172.16.0.0/16 is an extremely large range from 172.16.0.0 to 172.16.255.255. It is recommended not to discover ranges this large.
  - 10.255.0.0/23 is a moderately large range. This range goes from 10.255.0.0 to 10.255.1.255, and includes 512 IP addresses.
- Ranged input — IP address blocks are represented with a lowest-highest notation, for example 10.255.1.0 - 10.255.1.255. You can enter a single IP address, for example 192.168.100.1. Exclusion ranges can also be specified. This enables you to mask out certain addresses, or ranges of addresses, from network device detection. For example, you can scan the range 10.255.1.0/24. However, if there are printers from 10.255.1.10 to 10.255.1.20 that you do not want to scan, the inclusion range is 10.255.1.0/24. The exclusion range is 10.255.1.10 -10.255.1.20.

Field	Description/Action
Task Name	Displays Detect Network Devices. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Enter comments about the task.
Task Options	
Max Nodes	Enter the number of IP addresses to discover. The maximum is 1024. Keep in mind that tasks with more nodes than the maximum allowed will cause the task to fail.

Field	Description/Action
Inclusions	Enter IP addresses or Classless Inter-Domain Routing (CIDR) range inclusions (for example: 192.168.1.0-192.168.2.0 or 192.168.31.0/24) in right-hand box and click the << Add Discovery Range button. Ranges are inclusive. You can use the Delete Discovery Range button to delete ranges.
Exclusions	Enter IP addresses or Classless Inter-Domain Routing (CIDR) range exclusions (for example: 192.168.1.0-192.168.2.0 or 192.168.31.0/24) in the right-hand box and click the << Add Exclusion Range button. Ranges are inclusive. You can use the Delete Exclusion Range button to delete ranges.
Scanning Methods	Select one or both of the following scanning methods: • SNMP (the default) • Nmap (Note: Careful consideration should be taken when identifying the network range you are going to scan. Some network topologies can result in very long scans. In addition, it is recommended that you do not scan Internet addresses.) For detailed information on scanning methods, refer to “Scanning Methods” on page 344.
Password rule fallback	If selected (the default), SNMP scans the require community strings. Password rule fallback is used for those community strings.
Partitions	Select a Partition from the drop-down menu. Refer to “Segmenting Devices and Users” on page 150 for information on Partitions.
Device Group Name	Select one of the following options: • Use the default group name (DetectedNetworkDevices<*nnn*>, where *nnn* is the task ID) or select a device group from the drop-down menu. • Enter a device group name for added devices (the default). **Note**: When using the Detect Network Devices task, a new group could be created from devices that responded to the network scan, but did not return a known OS.
Driver Discovery	If checked (the default), device drivers are discovered after the device has been detected.
Device Credentials Options	
Device Credentials	Select one of the following options: • Use network-wide password rules • Use task specific credentials — Enter the username, password, and SNMP community string information.
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.

Field	Description/Action
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task schedule to be run a single time. Select the "Store log output generated by this task" checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to "Logging" on page 98 for detailed information on logging.

Be sure to click Save when you are finished.The Task Information page opens if the task is scheduled to run immediately. The Task Information page displays detailed information about the discovered nodes. Refer to "Task Information Page Fields" on page 408 for more information.

If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 399 for more information.

Deduplication Task Page Fields

If you import devices into NA using either the CSV (Comma Separated Value) file or Connectors, it is possible to have duplicate devices created in the NA database. For example, if you are importing devices from different management systems, such as HP Network Node Manager or CiscoWorks, they could use different management IP addresses to refer to the same device.

The Deduplication task enables you to resolve device duplication issues. Keep in mind that the Detect Network Devices task does this automatically. Refer to "Detect Network Devices Task Page Fields" on page 343 for information.

Field	Description/Action
Task Name	Displays Deduplication. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Applies to	Select one of the following options: • Device / Group — Enter an IP Address, Hostname, or Device Group name on which to run the task against or click the magnifying glass icon. For information on how to use the Device Selector, refer to "Device Selector" on page 144. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Enter comments about the task.

Field	Description/Action
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.

Field	Description/Action
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to “Logging” on page 98 for detailed information on logging.

Be sure to click Save when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task’s start date, duration, and status. Refer to “Task Information Page Fields” on page 408 for more information.

If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to “My Tasks Page Fields” on page 399 for more information.

OS Analysis Task Page Fields

The OS Analysis Task page collects data about the Cisco devices, such as Information about the sysoid (unique identifier for device model), OS version, flash storage options, modules, and so on. This information is then used to make software recommendations. After you run the OS Analysis task, click the “View the OS Recommendation for this device” link on the Task Information page. Refer to “Device Software Image Recommendation Page Fields” on page 225 for information.

Field	Description/Action
Task Name	Displays OS Analysis. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to “Task Templates” on page 282 for information on Task Templates.
Applies to	Select one of the following options: • Device / Group — Enter an IP Address, Hostname, or Device Group name on which to run the task against or click the magnifying glass icon. For information on how to use the Device Selector, refer to “Device Selector” on page 144. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to “Scheduling Tasks” on page 280 for information on task scheduling.
Comments	Enter comments about the task.
Task Options	
Session Log	To store the complete device session log, click the “Store complete device session log” check box. Keep in mind that all tasks that interact with a device can be run with session logging enabled. This provides a detailed log of the interaction with the device during the task. Session logs should be viewed as the first step to debugging device-specific issue. Session logs provide details on CLI, SNMP, and all transfer protocol actions taken during the task. (**Note**: Large amounts of data could be stored. Refer to “Logging” on page 98 for detailed information on logging.)

Field	Description/Action
Force Save	The device configuration update setting. This setting applies to only those devices that support a startup configuration. The default value of this setting is configurable per task type. • If NA should overwrite the startup configuration with the current running configuration at the completion of this task, select the Force Save check box. • If NA should not change the startup configuration, clear the Force Save check box. (**Note**: This setting is new in NA 9.20. It overrides all other approaches to determining whether to update the device startup configuration.)
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.

Field	Description/Action
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to “Logging” on page 98 for detailed information on logging.

Be sure to click Save when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task’s start date, duration, and status. Refer to “Task Information Page Fields” on page 408 for more information.

If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to “My Tasks Page Fields” on page 399 for more information.

Port Scan Page Fields

Nmap is used for discovering network devices. Nmap can also be used to scan a device's ports and return details on which ports are open and what services they provide. By running the Port Scan task, you can:

- Easily confirm which ports on a device are open or closed
- Determine a device's vulnerability based on TCP stack, OS detection, and other Nmap provided services

The results of the port scan are displayed on from the Device Details page's View menu (View --> Diagnostics --> NA Port Scan). Refer to "Device Details Page Fields" on page 195 for information on viewing device details.

To set Port Scan task settings, refer to "Device Access" on page 46.

Note: If the Port Scan task fails, it is possible that Nmap is not configured properly. Refer to "Device Access Page Fields" on page 47 for information on entering the path to the Nmap utility. For information on installing Nmap, see the *NA Installation and Upgrade Guide*.

Keep in mind that the ports are actually software based sockets open for listening. The details of the diagnostic are searchable using the Search for Diagnostics page. Refer to "Search For Diagnostic Page Fields" on page 501 for information.

Field	Description/Action
Task Name	Displays Port Scan. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Applies to	Select one of the following options: • Device / Group — Enter an IP Address, Hostname, or Device Group name on which to run the task against or click the magnifying glass icon. For information on how to use the Device Selector, refer to "Device Selector" on page 144. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.

Field	Description/Action
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Enter comments about the task.
Task Options	
Session Log	To store the complete device session log, click the "Store complete device session log" check box. Keep in mind that all tasks that interact with a device can be run with session logging enabled. This provides a detailed log of the interaction with the device during the task. Session logs should be viewed as the first step to debugging device-specific issue. Session logs provide details on CLI, SNMP, and all transfer protocol actions taken during the task. (**Note**: Large amounts of data could be stored. Refer to "Logging" on page 98 for detailed information on logging.)
Force Save	The device configuration update setting. This setting applies to only those devices that support a startup configuration. The default value of this setting is configurable per task type. • If NA should overwrite the startup configuration with the current running configuration at the completion of this task, select the Force Save check box. • If NA should not change the startup configuration, clear the Force Save check box. (**Note**: This setting is new in NA 9.20. It overrides all other approaches to determining whether to update the device startup configuration.)
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times

Field	Description/Action
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to “Logging” on page 98 for detailed information on logging.

Be sure to click Save when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task’s start date, duration, and status. Refer to “Task Information Page Fields” on page 408 for more information.

If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to “My Tasks Page Fields” on page 399 for more information.

Provision Device Task Page Fields

The Provision Device task applies a Device Template to a device. For information on creating Device Templates, refer to “Device Templates” on page 120.

Note: The task will fail if the Device Template and the device on which to apply it do not match.

Field	Description/Action
Task Name	Displays Provision Device. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to “Task Templates” on page 282 for information on Task Templates.
Applies to	Select one of the following options: • Device / Group — Enter an IP Address, Hostname, or Device Group name on which to run the task against or click the magnifying glass icon. For information on how to use the Device Selector, refer to “Device Selector” on page 144. • CVS File — Enter the name or browse for the CSV file containing a list of devices. If you click the Task CSV Template link, you can download a sample CSV file. Note that a CVS file is the only way to run a Provision Device task against multiple devices. It can also be used to assign a new Primary IP Address to the device after the task completes. Refer to “Edit Template Configuration Page” on page 122 for information.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to “Scheduling Tasks” on page 280 for information on task scheduling.
Comments	Enter comments about the task.
Task Options	
Session Log	To store the complete device session log, click the “Store complete device session log” check box. Keep in mind that all tasks that interact with a device can be run with session logging enabled. This provides a detailed log of the interaction with the device during the task. Session logs should be viewed as the first step to debugging device-specific issue. Session logs provide details on CLI, SNMP, and all transfer protocol actions taken during the task. (**Note**: Large amounts of data could be stored. Refer to “Logging” on page 98 for detailed information on logging.)

Field	Description/Action
Force Save	The device configuration update setting. This setting applies to only those devices that support a startup configuration. The default value of this setting is configurable per task type. • If NA should overwrite the startup configuration with the current running configuration at the completion of this task, select the Force Save check box. • If NA should not change the startup configuration, clear the Force Save check box. (**Note**: This setting is new in NA 9.20. It overrides all other approaches to determining whether to update the device startup configuration.)
Device Template	Select a device template from the drop-down menu.
Compliance option	If checked, NA will test policy compliance before provisioning the device.
Status option	If checked, the device status is set to Active upon provisioning.
Data copy option	If checked, additional information from the Device Template is copied to the device.
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.
Pre-Task / Post Task Snapshot Options	
Pre-Task Snapshot	Select one of the following options: • None • As part of task
Post-Task Snapshot	Select one of the following options: • None • As part of task • Scheduled as a separate task
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.

Field	Description/Action
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to “Logging” on page 98 for detailed information on logging.

Add Device Context Task Page Fields

A context is a device inside a device. A context can be hardware (with modules and slots) or virtual. As of NA 7.60, NA no longer requires that contexts have IP addresses. NA automatically discovers contexts on the parent device using the NA Module Status diagnostic. As part of the NA Module Status diagnostic, any contexts found are automatically added as devices and will have connection paths automatically configured. Refer to "New IP Address Page (New Connection Through)" on page 240 for information on connection through devices.

The NA Module Status diagnostic automatically adds internal device relationship as wells. For information on adding and removing user-defined device relationships, refer to "Device Relationships Page Fields" on page 228 for information.

In the case of the Cisco FWSM (Firewall Service Module), the CiscoFWSM is a module in a Cisco Catalyst device. The Cisco FWSM can include contexts. As a result, the Cisco FWSM and its contexts appear to NA as a device, since the Cisco FWSM and its contexts each have their own configurations.

Note: Instead of having to connect to a parent device and issuing a command to access a context, the NA device driver handles the connection to the context by connecting to the parent and automatically running the necessary scripts. As a result, the context appears as a standalone device.

When you run the NA Interfaces diagnostic, NA automatically discovers the contexts and adds the devices. When the NA Interfaces diagnostic sees a context has been removed, it marks the corresponding device as inactive. If the NA Interfaces diagnostic later sees the device, it will re-enable the device, thus preserving the device history.

Note: Removing a device context uses the same task page as when adding a device context. However, NA dynamically pulls the required variables from the driver.

Field	Description/Action
Task Name	Displays Add Device Context. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Applies to	Device — Enter an IP Address or Hostname on which to run the task against. Note that the device context tasks (add and remove) can only be run against a single device.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Enter comments about the task.
Task Options	
Session Log	To store the complete device session log, click the "Store complete device session log" check box. Keep in mind that all tasks that interact with a device can be run with session logging enabled. This provides a detailed log of the interaction with the device during the task. Session logs should be viewed as the first step to debugging device-specific issue. Session logs provide details on CLI, SNMP, and all transfer protocol actions taken during the task. (**Note**: Large amounts of data could be stored. Refer to "Logging" on page 98 for detailed information on logging.)
Force Save	The device configuration update setting. This setting applies to only those devices that support a startup configuration. The default value of this setting is configurable per task type. • If NA should overwrite the startup configuration with the current running configuration at the completion of this task, select the Force Save check box. • If NA should not change the startup configuration, clear the Force Save check box. (**Note**: This setting is new in NA 9.20. It overrides all other approaches to determining whether to update the device startup configuration.)

Field	Description/Action
Variables	Variables are defined in the device driver and displayed in NA at run-time. As a result, variables are different for each device. For the CiscoPIX FWSM device, there are three variables needed to create a device context: • Context Name —Enter the name of the device context you want to create. • Config Location — Enter the location of the configuration for the device context. In this case, it is a set of protocols that specify how you plan to provide the configuration. For example, if the configuration is on the local disk, you would select “disk” from the drop-down menu. • Config Filename — Enter the filename of the configuration, for example: default.cfg
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	Not available
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.

Field	Description/Action
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to “Logging” on page 98 for detailed information on logging.

VLAN Task Page Fields

NA enables you to provision VLAN entities and trunk ports. You can:

- Create new VLAN
- Edit a VLAN name
- Edit VLAN port assignments
- Edit VLAN comments (only in the database, not on the device)
- Configuring trunk ports (Refer to "Configuring Trunk Ports" on page 368 for information.)

Creating a new VLAN or editing VLAN names and port assignments on the New Device VLAN page results in scheduling a new VLAN task that performs the change on a device. Refer to "Creating and Editing VLANs" on page 218 for information.

Note: NA does not update the database with requested VLAN changes. Rather, NA schedules a post Snapshot task and a VLAN Data Gathering diagnostic task to capture the changes as the result of New VLAN task.

Field	Description/Action
Task Name	Displays Add VLAN. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Applies to	Device / Group — Enter an IP Address, Hostname, or Device Group name on which to run the task against or click the magnifying glass icon. For information on how to use the Device Selector, refer to "Device Selector" on page 144.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Enter comments about the task.

Field	Description/Action
Task Options	
Session Log	To store the complete device session log, click the "Store complete device session log" check box. Keep in mind that all tasks that interact with a device can be run with session logging enabled. This provides a detailed log of the interaction with the device during the task. Session logs should be viewed as the first step to debugging device-specific issue. Session logs provide details on CLI, SNMP, and all transfer protocol actions taken during the task. (**Note**: Large amounts of data could be stored. Refer to "Logging" on page 98 for detailed information on logging.)
Force Save	The device configuration update setting. This setting applies to only those devices that support a startup configuration. The default value of this setting is configurable per task type. • If NA should overwrite the startup configuration with the current running configuration at the completion of this task, select the Force Save check box. • If NA should not change the startup configuration, clear the Force Save check box. (**Note**: This setting is new in NA 9.20. It overrides all other approaches to determining whether to update the device startup configuration.)
Edit VLAN	Displays the name of the edited VLAN.
Rename to	Displays the new name of the VLAN.
Add ports	Displays the ports to add.
Remove ports	Displays the ports to delete.
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.

Field	Description/Action
Recurring Options	Not available
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the "Store log output generated by this task" checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to "Logging" on page 98 for detailed information on logging.

Configuring Trunk Ports

The VLAN Trunk option on the Edit Interface Detail page enables you to configure a trunk port. Keep in mind that only certain ports can be configured as trunk port, including physical ports and port channels (aggregated links). Loopback ports and ports that are used as VLAN interfaces cannot be configured as trunk ports.

The VLAN Trunk option is a collapsible set of rows that are displayed when you check the VAN Trunk option on the Edit Interface Detail page. The displayed fields include:

- Native VLAN ID
- Member VLANs

Native VLAN traffic is untagged on the trunk port. In addition, any untagged packets received on the trunk port are considered those of the Native VLAN.

Note: Native VLAN is a Cisco term. ProCurve does not use the Native VLAN term. Instead, ProCurve uses the Member VLANs term. As a result, the trunk port can have only one untagged VLAN membership. In essence, the Native VLAN ID and Member VLANs term have the same meaning.

Trunk ports carry the traffic of selected VLANs in the Member VLANs field. Any VLANs that are unselected will be pruned (removed the VLAN membership if the trunk ports were previously a member of the VLAN). Unchecking the VLAN Trunk option configures a port as a non-trunk port and assigns it to the VLAN indicated in the Native VLAN ID field.

Note: If the Trunk Port option is unchecked, you are prompted for the default VLAN ID if the port is currently a trunk port. The default VLAN ID is the one to which the port will be assigned when the trunk port becomes a non-trunk port. You are prompted to enter a VLAN ID. If you do not enter a VLAN ID, the Native VLAN ID will be used. If there is no Native VLAN ID, NA does not send the default VLAN ID to the device. As a result, the device will assign the port to its default VLAN, which is VLAN 1.

Refer to “Edit Interface Detail Page Fields” on page 210 for detailed information. Any modification of VLAN trunk port settings results in creating a VLAN task to apply the changes on the device. Refer to “VLAN Task Page Fields” on page 365 for information.

Download Image From Cisco.com Task Page

The Download Image From Cisco.com page enables you to browse Cisco.com Software Center to determine images that are available for download. The Cisco.com Software Center contains released versions of system software and drivers for Cisco's internetworking products.

To open the Download Image From Cisco.com page, on the menu bar under Devices, select Device Tools and click Software Images. The Software Images Page opens. Click the Add Image Set From Cisco.com link at the top of the page.

Field	Description/Action
Task Name	Displays Download Image From Cisco.com. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to “Task Templates” on page 282 for information on Task Templates.
Applies to	Select one of the following options: • Device / Group — Enter an IP Address, Hostname, or Device Group name on which to run the task against or click the magnifying glass icon. For information on how to use the Device Selector, refer to “Device Selector” on page 144.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Comments	Enter comments about the task.
Task Options	
Modify Device/Group List	When you click the Refresh Device List button, any devices selected above will be listed in the Device List field if Cisco is the device vendor. If a device from another vendor is selected, it will not be displayed in the Device List field. Generic platform information is also displayed. This enables you to find software images for devices that you plan to use in the future or have not yet added to NA. There is a flow between the following fields when you select an item in the Device List field. Refer to “Device Software Image Recommendation Page Fields” on page 225 for detailed information on the following fields. • Device List — Lists all available generic Cisco devices. • Version List — Displays device version information for the selected device. • Feature List — Displays feature information for the selected device.
Download Selection	Select the software image you want to download and click the Save Task button. Refer to “Add Software Image Set Page Fields” on page 447 for information.

Field	Description/Action
Apply to Partition	Select a Partition from the drop-down menu. (**Note**: This field is only displayed if you have configured one or more Partitions.) If you have created Partitions for security or business reasons, you can partition software images according to Partitions. If the software image is available to all Partitions, the software image is labeled “Shared” (or “Global”) depending on configuration.
Scheduling Options	
Retry Count	Not available
Recurring Options	Not available
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to “Logging” on page 98 for detailed information on logging.

Be sure to click the Save button when you are finished. The Task Information page opens. The page includes detailed task information, including task status, devices affected, duration, result details, and so on.

Backup Device Software Task Page Fields

The Backup Device Software task enables you to copy software images from a device(s) to the NA software image repository. All copied software images are added to an existing software image set unless you specify that each software image goes in its own unique software image set. The name of the software image set then becomes a combination of the specified software image set name and the name of the software image set copied from the device. Keep in mind:

- A new software image set name is created if you specify a unique name.
- Software image sets are added to an existing software image set if the software image set name is not unique.
- Duplicate software images are not added to an existing software image set. As a result, you will receive a warning message when the Backup Device Software task runs.

When a new software image set is created, the attributes of the software image set match information known about the device from which it was downloaded. This ensures that the downloaded software images are not applied to devices that are not capable of running the software image. Refer to "Image Synchronization Report Fields" on page 624 for information.

A link is provided on the Backup Device Software Task Results page to a list of the software image set(s) so you can verify all software image set names and requirements

To open the Backup Device Software Task page, on the menu bar under Reports, select Image Synchronization Report. On the Image Synchronization Report, check one or more checkboxes and then select the Sync Image option from the Actions drop-down menu.

Field	**Description/Action**
Task Name	Displays Backup Device Software. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Enter comments about the task.
Custom 1	Enter custom data.

Field	Description/Action
Task Options	
Session Log	To store the complete device session log, click the "Store complete device session log" check box. Keep in mind that all tasks that interact with a device can be run with session logging enabled. This provides a detailed log of the interaction with the device during the task. Session logs should be viewed as the first step to debugging device-specific issue. Session logs provide details on CLI, SNMP, and all transfer protocol actions taken during the task. (Note: Large amounts of data could be stored. Refer to "Logging" on page 98 for detailed information on logging.)
Force Save	The device configuration update setting. This setting applies to only those devices that support a startup configuration. The default value of this setting is configurable per task type. • If NA should overwrite the startup configuration with the current running configuration at the completion of this task, select the Force Save check box. • If NA should not change the startup configuration, clear the Force Save check box. (**Note**: This setting is new in NA 9.20. It overrides all other approaches to determining whether to update the device startup configuration.)
Base Image Set Name	You can select from the following options: • Use Name — Enter the base image set name. • Use Existing — Select an existing software image set from the drop-down menu.
Image Storage	The device and software image you are copying to the NA software respository are displayed. You can select from the following options: • Group Image Sets — All copied software images are added to either a new or existing software image set. • Separate images into unique Image Sets — The image set name specified above (either manually or selected) is used as the base name for the new image set. The full name will include the original name and the name of the software image copied from the device.
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	This option is not available for this task.

Field	Description/Action
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to “Logging” on page 98 for detailed information on logging.

Be sure to click the Save Task button when you are finished. The Task Information page opens. The page includes detailed task information, including task status, devices affected, duration, result details, and so on.

Check Policy Compliance Task Page Fields

The Check Policy Compliance task enables you to determine if devices are in compliance with either configuration policies or software level policies. You should only need to run the Check Policy Compliance task when you create or update policies. By doing so, you can quickly determine if a device is out of compliance with the newly created policy.

Note: By default, NA runs a compliance check on a device's configuration whenever a configuration change is detected. If configured, you are notified if a configuration change violates applied policies. In addition, you can configure a number of automated reactions, such as emailed alerts, SNMP traps, and even run a command script to force the device to return to a compliant state.

Field	Description/Action
Task Name	Displays Check Policy Compliance. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Applies to	Select one of the following options: • Device / Group — Enter an IP Address, Hostname, or Device Group name on which to run the task against or click the magnifying glass icon. For information on how to use the Device Selector, refer to "Device Selector" on page 144. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Enter comments about the task.

Field	Description/Action
Task Options	
Action	Select one or all of the following options: • Check configuration policy compliance (the default) — Checks to see if the selected device(s) are in compliance with configuration policies. • Check diagnostics compliance — Checks to see if the selected device(s) are in compliance with diagnostic policies. • Check software compliance — Checks to see if the selected device(s) are in compliance with software policies. • Check software level — If checked, the software level is checked, resulting in text output showing the software level and any identified security vulnerabilities.
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.

Field	Description/Action
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to “Logging” on page 98 for detailed information on logging.

Be sure to click Save when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task’s start date, duration, and status.

Refer to “Task Information Page Fields” on page 408 for more information. If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to “My Tasks Page Fields” on page 399 for more information.

Generate Summary Reports Task Page Fields

The Generate Summary Reports task enables you to update the Summary reports (which by default are updated by a recurring task each Sunday). If you want to permanently change the schedule for updating Summary reports, you can edit the existing recurring task.

Field	Description/Action
Task Name	Displays Generate Summary Reports. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the magnifying glass icon to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Enter comments about the task.
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times

Field	Description/Action
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.

Be sure to click Save when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status. Refer to "Task Information Page Fields" on page 408 for more information.

If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 399 for more information.

Email Report Task Page Fields

The Email Report task enables you to email NA reports.

Field	Description/Action
Task Name	Displays Email Report. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Enter comments about the task.
Task Options	
Report to run	Select a report to email. Keep in mind that each time this task runs, the last saved report is overwritten with the new information. (**Note**: Summary reports cannot be emailed using this task.)
Applies to	This field is displayed for the Network Status report only. Select the device group against which you want to run the report.
Email Recipients	Enter one or more email addresses. Be sure to separate addresses with commas.
Email Subject	Enter the subject line of the email message.
Email Format	Select one of the following options from the drop-down menu: • Default format • HTML mail • CSV file attachment • Plain text • HTML mail (without links)
File Export	Click the check box to save a copy of the report to file.

Field	Description/Action
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.

Field	Description/Action
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to “Logging” on page 98 for detailed information on logging.

Be sure to click Save when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task’s start date, duration, and status. Refer to “Task Information Page Fields” on page 408 for more information. If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to “My Tasks Page Fields” on page 399 for more information.

Deploy Remote Agent Page Fields

The Deploy Remote Agent task enables you to deploy a NA remote agent on each Satellite Gateway host. By installing a NA remote agent on the same LAN with the devices being managed, WAN traffic can be minimized and Syslog and TFTP can be used to manage the devices locally.

To open the Deploy Remote Agent task, on the menu bar under Tasks, select New Task and click Deploy Remote Agent. You can also navigate to this page by clicking the Deploy Remote Agent link on the Gateway List page. Refer to "Gateway List Page Fields" on page 155 for information.

Field	Description/Action
Task Name	Displays Deploy Remote Agent. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Enter comments about the task.
Task Options	
Action	Select one of the following options: • Install (or Reinstall) — Installs the NA remote agent. If there is already a NA remote agent installed, the existing NA remote agent is removed and a new NA remote agent is installed. • Uninstall — Uninstalls the NA remote agent.
Deploy Agent to Gateway	Select the Gateway name from the drop-down menu where the NA remote agent is to be deployed.
Login	Deploying a remote agent requires root privileges on the Satellite Gateway host. Select one of the following options: • As Root — SSH as username root and enter the root password. • As Non-root — SSH as a non-root user. If you select this option, select either su Password (the root password) or sudo Password (the sudo password, which is typically the same as your username password, but can be different depending on how sudo is configured).

Field	Description/Action
Managing Core	If the Core Gateway is installed on the same host as the NA Core, the Managing Core should be “localhost” (the default). If the Core Gateway is on a different host from the NA Core, the Managing Core should be the hostname or IP Address of the NA Core. (**Note**: If the NA Core host has a different IP address, use the IP address that is appropriate when connecting to the NA Core from the Core Gateway host.)
In Realm	Select the Realm name of the Core Gateway from the drop-down menu.
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	Not available
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to “Logging” on page 98 for detailed information on logging.

Resolve FQDN Task Page Fields

The Resolve FQDN task enables you to set the FQDN (Fully Qualified Domain Name) for each device in the system by running a reverse DNS lookup on the device's primary IP address.

Field	Description/Action
Task Name	Displays Resolve FQDN. You can enter a different task name if applicable.
Save Options	Select one or more of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Applies to	Select one of the following options: • Device / Group — Enter an IP Address, Hostname, or Device Group name on which to run the task against or click the magnifying glass icon. For information on how to use the Device Selector, refer to "Device Selector" on page 144. • CSV — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file. **Note**: When scheduling tasks to run against an ad-hoc device group (by using the check boxes on the Device List page to select devices for the group), this section displays the devices included in the ad-hoc device group.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Enter comments about the task.
Task Options (not available)	
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.

Field	Description/Action
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to “Logging” on page 98 for detailed information on logging.

Be sure to click Save when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status. Refer to "Task Information Page Fields" on page 408 for more information. If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 399 for more information.

Data Pruning Task Page Fields

Data pruning is a system task that requires a system administrator or someone with similar permissions to configure the system. Data pruning removes obsolete files, diagnostics, events, and tasks. The following files are not removed by data pruning:

- Current configuration
- Configurations scheduled for deployment

When the NA server is configured for pruning, you can specify how long the files should be kept. The default settings for these files include:

- Configurations — 365 days
- Tasks — 365 days
- Diagnostics — 45 days
- Events — 45 days
- Sessions — 45 days
- Log files — 30 days

Field	Description/Action
Task Name	Displays Data Pruning. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Enter comments about the task.
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.

Field	Description/Action
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to “Logging” on page 98 for detailed information on logging.

Be sure to click Save when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task's start date, duration, and status.

Refer to "Task Information Page Fields" on page 408 for more information. If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to "My Tasks Page Fields" on page 399 for more information.

Run External Application Task Page Fields

The Run External Application task enables you to schedule an external application to run from NA, such as the "ping" command or an external language interpreter. This task can be used to enable integration with external Help Desk and NMS solutions.

Note: On a Windows platform, the path should use the Windows file separator character, which is a backslash (\). The short names (those with ~<*n*>) are only needed when a file name includes spaces. For example, *C:\Rendition* is fine, but *C:\Program Files* is not. Keep in mind that short names are only needed when you are passing parameters, for example: *C:\Program Files\Internet Explorer\iexplore.exe* is fine. However, *C:\Program Files\Internet Explorer\iexplore.exe someFilename.html* will not work. You would need to use *C:\Progra~1\Intern~1\iexplore.exe someFilename.html*.

Field	Description/Action
Task Name	Displays Run External Application. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Enter comments about the task.
Task Options	
Run	Enter the command line utility or script you want to execute. Be sure to provide the fully-qualified path and filename for the executable file. You can supply parameters to an external application by supplying both the name of the application to run, followed by its parameter(s). For example, to run an external command "foo" with parameters "bar" and "bat", you would enter "foo bar bat" without the quotes.
Start in	Enter the path of the external application and the startup directory for that application.
Task Result	Check the "Treat non-zero result code as fail task" box if you want to treat non-zero result code as a failed task.

Field	Description/Action
Text Output	Select one of the following options: • Results from stdout (the default) — After the application runs, its standard text output to the console is stored in the Task Details. This is used for most applications, such as command line utilities. • Results from file — For no output, select this option, but leave the filename blank. After the application runs, NA reads this file and includes the contents in the Task Details. This is useful for commands that write output to a file instead of stdout. Be sure to enter the fully-qualified path to the result file, if applicable.
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.

Field	Description/Action
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon task completion, select the Email Notification check box. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.
Task Logging	
Task Logging	If available, you can enable logs for a specific task scheduled to be run a single time. Select the “Store log output generated by this task” checkbox and select one or more logs using the Shift key. The logs you select are highlighted. Keep in mind when a task has been setup to run with logging, and the log is not able to be initiated, the task will fail immediately without any further processing. Refer to “Logging” on page 98 for detailed information on logging.

Be sure to click Save when you are finished. The Task Information page opens if the task is scheduled to run immediately. The Task Information page provides task details, such as the task’s start date, duration, and status. Refer to “Task Information Page Fields” on page 408 for more information.

If the task is scheduled to start in the future, the My Tasks page opens with the new task highlighted. Refer to “My Tasks Page Fields” on page 399 for more information.

Scheduling Multi-Task Projects

You can configure a multi-task project to run several different tasks sequentially joined together under a single project. For example, you might want to perform a software upgrade and then push an updated configuration to the device. Consolidating the tasks together under one project simplifies the management approvals by authorizing work at the project level rather than the task level. It also enables you to coordinate sets of disparate tasks and manage them as one unit.

Note: You must have the proper permissions to run Multi-Task Projects. Refer to "User Roles & Permissions Page Fields" on page 259 for information.

Each task included in the multi-task project is run in the order you specify. For example, you can schedule driver discovery, a snapshot, run a custom script, and so on, for a group of devices. Keep in mind that as far as the NA Scheduler is concerned, the multi-task project is considered one task. When the multi-task project is scheduled to run, the NA Scheduler runs all the tasks in the order specified. If for some reason one of the tasks in the multi-task project does not run, the multi-task project fails. If the multi-task project requires approval, when the multi-task project is approved, all of the tasks included in the multi-task project are automatically approved.

Note: You can reserve devices and/or device groups using the Multi-Task Project page.

Sub-task Warning Status

For multi-task projects, if a sub-task completes with a Warning status, you can continue to run subsequent sub-tasks or cancel all of the remaining sub-tasks. This feature enables you to cancel tasks that are running against a device that could be experiencing issues.

To enable this feature:

1. From the Admin menu, navigate to the Custom Data Setup page.
2. Scroll down to the 6th API Name field under the Tasks section.
3. In the 6th API Name field, enter: **subtask_control**
4. In the Display Name field, enter: **Cancel remaining tasks that have warning message**
5. In the Values field, check the Limit to: checkbox and enter: **Yes**, **No**
6. Click the Save button.

If this feature is enabled, when you create sub-tasks for multi-task projects, the following field is displayed under the Comments field on all multi-task sub-task pages: `Cancel remaining tasks that have warning messages`

This field includes the following options:

- Blank — The remaining sub-tasks continue to run.
- Yes — The remaining sub-tasks are canceled.
- No — The remaining sub-tasks continue to run.

Note: To disable this feature, uncheck the 6th API Name checkbox on the Custom Data Setup page and click the Save button.

To create a multi-task project, on the menu bar under Tasks, click New Multi-Task Project. The New/Template Task - Multi-Task Project page opens.

Multi-Task Project Page Fields

Field	Description/Action
Task Name	Displays Multi-Task Project. You can enter a different task name if applicable.
Save Options	Select one of the following options: • Save as task — The option is selected by default. • Save as task template — If selected, the task is saved as a task template and displayed on the Tasks Templates page. Refer to "Task Templates" on page 282 for information on Task Templates.
Start Date	Select one of the following options: • Start As Soon As Possible (the default) • Start At — Enter a date and time to start the task. Click the calendar icon next to the date box to open the calendar and select a date and time.
Task Priority	Enables you to set a priority for the task. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks. Refer to "Scheduling Tasks" on page 280 for information on task scheduling.
Comments	Add any comments about the multiple task job.
Task Options	
Sub Tasks	Select a subtask from the drop-down menu. Depending on the subtask you select, the new task page for that task opens, where you can configure the task. For example, if you select the Configure Syslog task, the New Task - Configure Syslog page opens. As you add tasks, they are displayed on the Edit Task - Multiple Task Project page. You can edit or delete the task if necessary. When you click Save Task, the Pending Tasks page opens. Refer to "Scheduled Tasks Page Fields" on page 402.
Reserved Devices	Use the Device Selector to reserve devices. For information on how to use the Device Selector, refer to "Device Selector" on page 144 or click the question mark (?) in the upper right-hand corner of the Device Selector.
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that the tasks are to run against. The default is 60 minutes.
Approval Options	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.

Field	Description/Action
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	Not available
Task Completed Notficiation	
Task Completed Notification	If you want NA to send an email message upon completion of the multi-task project, select the Email Notification check box. **Note**: NA does not send an email message upon completion of each subtask. **Tip**: The format of the email content is the same for all tasks. For information about changing the email content, see the *NA Administration Guide*.
Email Recipients	Enter a comma-separated list of email addresses to receive the message. The default value is the email address of the task originator.

When you are finished, be sure to click Save.

How to Configure a Multi-Task Project

This section steps you through the process of setting up a multi-task project, including reserving devices and/or device groups for your project and using the Activity Calendar to view your project's reserved devices and/or device groups.

1. On the menu bar under Tasks, click New Multi-Task Project. The New Task/Template - Multi-Task Project page opens.
2. In the Task Name field, enter a name for your project, for example Pine Valley Office. It is assumed that you have already added specific devices and/or device groups to a parent group named *Pine Valley Office*. If not, refer to “Adding Device Groups” on page 138 for information.
3. In the Start Date field, either check Start As Soon As Possible (the default) or click the calendar, from which you can select a date and time you want your project to start.
4. Click the down arrow to select a task priority from 1 to 5, with 1 being the highest priority. The default value is 3. Higher priority tasks run before lower priority tasks.
5. In the Comments field, enter comments about your project.
6. In the Sub Tasks field under Task Options, select a sub-task you want to include in your project from the drop-down menu. For example, if you select the Deploy Passwords task, the New Task/Template - Deploy Passwords page opens.
7. Using the Deploy Passwords page, in the Applies To field, select Pine Valley Office from the drop-down menu. You could also enter the name or browse for a CSV file containing a list of the devices and/or device groups in Pine Valley Office.
8. Complete the Task Options section. The options displayed in this section differ from task to task. For information on the Deploy Password task, refer to “Deploy Passwords Task Page Fields” on page 290.
9. Click Save Task. You are returned to the Multi-Task Project page, where you can add additional sub-tasks to your project.
10. To reserve all of the devices in the Pine Valley Office, in the Reserved Devices field, click Modify. The Device Selector opens.
11. Double click Pine Valley Office. All devices in the Pine Valley Office are displayed.
12. If you want to reserve all of the devices in the Pine Valley Office, click Select All and then click the right arrows (>>>). The devices are listed in the Selected Devices box. To add only specific devices, you can narrow your search by entering a portion of the host name or IP address of the device or select only devices you want to add, and then click the right arrow.
13. Enter the Estimated Duration time for which you want to reserve the devices. The default is one hour.
14. Click Save Task. The list of reserved devices is included in the Reserved Devices field.
15. Click Save Task. The My Tasks page opens, where you can edit, delete, pause, or run your project immediately.
16. On the menu bar under Tasks, click Activity Calendar. The Activity Calendar opens.

17. Using the calendar, select the day on which your project has reserved the Pine Valley Office devices. Your project, Pine Valley Office, is displayed in the time slot you selected.
18. Click Pine Valley Office. The Task Information page opens, where you can view detailed information about your project.

Viewing My Tasks

The My Tasks page shows tasks originated by the currently logged in user, including the task approval status, if applicable, and if the task has not yet run.

To view the My Task page, on the menu bar under Tasks, click My Tasks. The My Task page opens.

My Tasks Page Fields

Field	Description/Action
My Drafts link	If applicable, opens the My Drafts page.
Approval Requests link	If the task requires approval, opens the Approval Requests page, where you can view tasks needing approval by the currently logged in user. By default, the page shows tasks that have not completed, including tasks that are: • Not approved • Waiting Approval • Waiting to run Refer to "Approval Requests" on page 676 for information.
Scheduled Tasks link	Opens the Scheduled Tasks page, where you can view scheduled tasks that are in the queue, but have not yet run. Refer to "Scheduled Tasks Page Fields" on page 402 for information.
Running Task link	Opens the Running Task page, where you can view all running tasks. Refer to "Running Tasks Page Fields" on page 404 for information.
Recent Tasks link	Opens the Recent Tasks page, where you can view all recent tasks. Refer to "Recent Tasks Page Fields" on page 406 for information.
Show Tasks Check Boxes	If the task requires approval, you can select the following display options: • Approved • Not Approved • Waiting Approval • Overridden • Draft • No Approval Required
Check Boxes	You can use the left-side check boxes to delete tasks. Once you have selected the tasks, click the Actions drop-down menu and click Delete. The adjacent Select drop-down menu enables you to select or deselect all tasks.
Schedule Date	Displays the date and time the task was created.
Approved By Date	If applicable, displays the date and time the task must be approved. If a task is not approved by its approval date, its status is set to "Not Approved." (**Note**: Approval options are only displayed if the task is part of a Workflow Approval Rule.)

Field	Description/Action
Task Name	Displays the task name. Clicking a task opens the Task Details page. Refer to "What Are Tasks?" on page 279 for information.
Approval Status	If applicable, displays the task's approval status. Approval status is only displayed if the task is part of a Workflow Approval Rule. Approval statuses include: • Awaiting Approval • Approved • Not Approved • Overridden • No Approval Required
Task Status	Displays the status of the task. Statuses include: • Warning — A group task containing some failed sub-tasks, but not all tasks failed. • Draft — NA will not run the task, nor is the task sent out for approval, when in Draft status. • Duplicate — The task was not started because an identical task is already running. • Failed — The task failed. • Paused — Someone paused the task. It will not run when its scheduled time arrives. • Pending — The task is queued and waiting for its scheduled time. • Running — The task has started, but has not yet finished. • Skipped — The task was skipped due to errors, for example incorrect permissions, unmanaged devices, and so on. • Succeeded — The task succeeded. • Waiting — Although the scheduled time has arrived, the task is waiting because the "Max Concurrent Tasks" limit has been reached.
Priority	Displays the task's priority. There are five task priority levels, 1 through 5. 1 is the highest task priority level. Refer to "Scheduling Tasks" on page 280 for more information.
Task Type	Displays the task type, for example: • Deploy Password • Deploy Config • Discover Driver • Reboot Device • Take Snapshot • Synchronize Startup and Running Configurations For a complete list of tasks, refer to "What Are Tasks?" on page 279. (**Note**: Multi-Task Project tasks may or may not be displayed on the My Tasks results page. It depends on whether the Multi-Task Project task includes at least one of the task types listed above as a sub-task.)

Field	Description/Action
Actions	Select one of the following options: • Delete — Enables you to delete the task. • Pause — Pauses the task so it does not run at its scheduled time. (**Note**: You can select Resume if you want to resume the task.) • Run Now — Runs the task as soon as possible. If the maximum number of concurrent tasks has not been reached, the task runs immediately. • Edit — Opens the Edit Task page.
Display results in groups of	You can set the number of items to display per page from the drop-down menu. The default is 25.

Viewing Scheduled Tasks

To view scheduled tasks that are in the queue, but have not yet run, on the menu bar under Tasks click Scheduled Tasks. The Scheduled Tasks page opens.

Note: To change the task page refresh interval, on the menu bar under Admin, select Administrative Settings and click User Interface. On the User Interface page, scroll down to the Miscellaneous section and enter a task page refresh interval.

Scheduled Tasks Page Fields

Field	Description/Action
My Tasks link	Opens the My Task page. Refer to "My Tasks Page Fields" on page 399 for information.
Task Templates link	Opens the Task Template page. Refer to "Task Templates" on page 282 for information.
My Drafts link	Opens the My Drafts page. Refer to "My Tasks Page Fields" on page 399 for information.
Approval Requests link	If the task requires approval, opens the Approval Requests page, where you can view tasks needing approval by the currently logged in user. Refer to "Approval Requests" on page 676 for information.
Running Task link	Opens the Running Task page. Refer to "Running Tasks Page Fields" on page 404 for information.
Recent Tasks link	Opens the Recent Tasks page. Refer to "Recent Tasks Page Fields" on page 406 for information.
Current Working Group	Displays the name of the current working group. You can select a different group from the drop-down menu and click the Refresh button.
Show Group/Parent Tasks Only	If checked, only group and parent tasks are shown.
Check Boxes	You can use the left-side check boxes to delete scheduled tasks. Once you have selected the tasks, click the Actions drop-down menu and click Delete. The adjacent Select drop-down menu enables you to select or deselect all tasks.
Schedule Date	Displays the date and time when NA is scheduled to run the task.
Task Name	Displays the task name.
Host/Group	Displays the host or group name of the network device(s) associated with the task. You can click the link to open the Device Information page, where you can view basic information about the devices in the group.

Field	Description/Action
Task Status	Displays the status of the task, for example: • Pending — The task is queued, but has not yet run. • Paused — Polling is paused. To resume polling, enter the “resume polling” CLI command. • Draft — The task is in Draft mode and will not run. For a complete list of task statuses, refer to “Task Information Page Fields” on page 408.
Priority	Displays the task’s priority. There are five task priority levels, 1 through 5. 1 is the highest task priority level. Refer to “Scheduling Tasks” on page 280 for more information.
Scheduled By	Displays the login name of the person who scheduled the task (or the last user to modify the task).
Comments	Displays comments about the pending task.
Actions	You can select the following actions for each entry in the Pending Tasks table: • Delete — Deletes the task. • Pause — Pauses the task so it does not run at its scheduled time. (**Note**: You can select Resume if you want to resume the task.) • Run Now — Runs the task as soon as possible. If the maximum number of concurrent tasks has not been reached, the task runs immediately. • Edit — Opens the Edit Task page, where you can edit and rerun the task that is recurring or has not yet occurred. • Create Template — Opens the Task Templates page, where you can save task definitions so that you can easily configure and run new and existing tasks without having to start from scratch. Refer to “Task Templates” on page 282 for information.
Display results in groups of	You can set the number of items to display per page from the drop-down menu. The default is 25.

Viewing Running Tasks

To view running tasks, on the menu bar under Tasks click Running Tasks. The Running Tasks page opens.

Note: To change the task page refresh interval, on the menu bar under Admin, select Administrative Settings and click User Interface. On the User Interface page, scroll down to the Miscellaneous section and enter a task page refresh interval.

Running Tasks Page Fields

Field	**Description/Action**
My Tasks link	Opens the My Task page. Refer to "My Tasks Page Fields" on page 399 for information.
My Drafts link	Opens the My Drafts page. Refer to "My Tasks Page Fields" on page 399 for information.
Approval Requests link	Opens the Approval Requests page, where you can view tasks needing approval by the currently logged in user. Refer to "Approval Requests" on page 676 for information.
Scheduled Task link	Opens the Scheduled Task page. Refer to "Scheduled Tasks Page Fields" on page 402 for information.
Recent Tasks link	Opens the Recent Tasks page. Refer to "Recent Tasks Page Fields" on page 406 for information.
Current Working Group	Displays the current working group. Use Ctrl+click to select/deselect more than one group.
Show Child Tasks	To include child and parent tasks in the list of running tasks, select this check box. To include only parent tasks in list of running tasks, clear this check box.
Refresh this page every 60 seconds	Uncheck this box if you do not want the display to refresh every 60 seconds. Refer to "User Interface Page Fields" on page 63 for information on setting this value.
Check Boxes	You can use the left-side check boxes to delete tasks. Once you have selected the tasks, click the Actions drop-down menu and click Delete. The adjacent Select drop-down menu enables you to select or deselect all tasks.
Start Date	Displays the date and time NA began running the task.
Task Name	Displays the task type.
Host/Group	Displays the host or group name of the network device(s) associated with the task. You can click the link to open the Device Information page, where you can view basic information about the devices in the group.
Task Status	Displays the status of the task (running). If the maximum number of concurrent tasks has been reached, the task is waiting for another task to finish. Consequently, the Running Tasks page returns "No Tasks Found." (**Note**: The number of tasks could exceed the Max Concurrent Tasks value because group parent tasks are not included in the setting.)

Field	Description/Action
Priority	Displays the task's priority level. Refer to "Scheduling Tasks" on page 280 for information on setting task priority.
Core	In a Horizontal Scalability environment, displays the name of the NA core on which the task is running.
Partition	If NA uses partitions, displays the name of the partition in which the task is running. Refer to "Segmenting Devices and Users" on page 150 for detailed information on creating Partitions.
Scheduled By	Displays the login name of the person who scheduled the task (or the last user to modify the task).
Comments	Displays comments about the pending task.
Actions	Available actions include: • Detail — Opens the Task Information page, where you can view details about the task. • Cancel — Cancels the task. • Increase Priority — If your NA user is authorized to do so, increases the task's priority level. Available for parent tasks only. • Decrease Priority — Decreases the task's priority level. Available for parent tasks only.
Display results in groups of	You can set the number of items to display per page from the drop-down menu.

Viewing Recent Tasks

To view recent tasks, on the menu bar under Tasks click Recent Tasks. The Recent Tasks page opens. The Recent Tasks page shows all recent tasks, regardless of their status.

Note: To change the task page refresh interval, on the menu bar under Admin, select Administrative Settings and click User Interface. On the User Interface page, scroll down to the Miscellaneous section and enter a task page refresh interval.

Recent Tasks Page Fields

Field	Description/Action
My Tasks link	Opens the My Task page. Refer to "My Tasks Page Fields" on page 399 for information.
Task Templates link	Opens the Task Template page. Refer to "Task Templates" on page 282 for information.
My Drafts link	Opens the My Drafts page. Refer to "My Tasks Page Fields" on page 399 for information.
Approval Requests link	Opens the Approval Requests page, where you can view tasks needing approval by the currently logged in user. Refer to "Approval Requests" on page 676 for information.
Scheduled Tasks link	Opens the Scheduled Task page. Refer to "Scheduled Tasks Page Fields" on page 402 for information.
Running Tasks link	Opens the Running Tasks page. Refer to "Running Tasks Page Fields" on page 404 for information.
Current Working Group	Displays the group name of the network device(s) associated with the task. Use Ctrl+click to select/deselect more than one group.
Show Tasks Within	Select the time frame for which to view recent tasks, and then click Refresh.
Show Detail	To view task details for the recent tasks, select this check box, and then click Refresh.
Show Child Tasks	To include child and parent tasks in the list of recent tasks, select this check box, and then click Refresh. To include only parent tasks in list of recent tasks, clear this check box, and then click Refresh.
Task Status	Select the task statuses to display, and then click Refresh.
Check Boxes	You can use the left-side check boxes to delete tasks. Once you have selected the tasks, click the Actions drop-down menu and click Delete. The adjacent Select drop-down menu enables you to select or deselect all tasks.
Complete Date	Displays the date and time NA began running the task.
Task Name	Displays the task type.

Field	Description/Action
Host/Group	Displays the host or group name of the network device(s) associated with the task. You can click the link to open the Device Information page, where you can view detailed information about the devices in the group.
Task Status	Displays the status of the task, for example: • Succeeded — The task succeeded. • Failed — The task failed. • Duplicate — The task duplicated another task. • Skipped — The task was skipped because an identical task was already running when the time arrived for this task to run. For a complete list of task statuses, refer to "Task Information Page Fields" on page 408.
Priority	Displays the task's priority. There are five task priority levels, 1 through 5. 1 is the highest task priority level. Refer to "Scheduling Tasks" on page 280 for more information.
Core	In a Horizontal Scalability environment, displays the name of the NA core on which the task ran.
Partition	If NA uses partitions, displays the name of the partition in which the task ran. Refer to "Segmenting Devices and Users" on page 150 for detailed information on creating Partitions.
Scheduled By	Displays the login name of the person who scheduled the task (or the last user to modify the task).
Comments	Displays comments about the task.
Actions	You can select the following action for each task in the Recent Tasks table: • Detail — Opens the Task Information page, where you can view details about the task. • Run Again — Opens the Rerun Task page, where you can edit the task and run it again. (**Note**: This option only appears if the task can be rerun.) • Create Template — Opens the Task Templates page, where you can save task definitions so that you can easily configure and run new and existing tasks without having to start from scratch. Refer to "Task Templates" on page 282 for information.
Display results in groups of	You can set the number of items to display per page from the drop-down menu.

Task Information Page Fields

The Task Information page includes detailed information on tasks, including:

- Task status
- Task priority
- Originator
- Devices affected
- Duration
- Approval information
- Result details
- Task history

The Task information page also provides links to more detailed information in the event of a warning or failure. Keep in mind that a task can be successfully completed but still contain errors. For example, you could successfully deploy to a running configuration but have invalid commands within the configuration.

To open the Task Information page:

1. Select a device from the Inventory page. The Device Details page opens.
2. From the View drop-down menu, click Device Tasks. The Device Tasks page opens.
3. Click the Detail option in the Actions column for the task on which you want detailed information. The Task Information page opens.

Field	Description/Action
Edit Task link	Opens the task page so that you can edit the task. This link is only displayed for pending tasks. Refer to "What Are Tasks?" on page 279.
Run Again link	Opens the task page so that you can re-run the task. This link is only displayed for completed tasks. Refer to "What Are Tasks?" on page 279.
Return to List link	Opens the My Tasks page. Refer to "Viewing My Tasks" on page 399.
General Information	
Task Name	Displays the task name.

Field	Description/Action
Task Status	Displays the task status, including: • Draft • Duplicate • Failed • Paused • Pending • Requested (Note: Requested means the task is waiting for Approval. Refer to "Approving Tasks" on page 678.) • Running • Skipped • Succeeded • Synchronous (**Note**: NA typically runs tasks by creating a thread and letting the task run asynchronously in the background. The CLI and API enable synchronous tasks where they are run in the current thread and the command blocks until the command completes.) • Waiting • Warning **Note**: Multi-task projects will continue processing when a warning is encountered. The warning status is shown in the parent task.
Comments	Displays any comments about the task.
Originator	Displays the username or process that scheduled the task.
Priority	Displays the task's priority. There are five task priority levels, 1 through 5. 1 is the highest task priority level. Refer to "Scheduling Tasks" on page 280 for more information.
Create Date	Displays the date and time the task was created.
Devices Affected	Displays the host name and/or IP address of the affected device.
Schedule Date	Displays the date and time the task was scheduled to run.
Start Date	Displays the task's start date.
Complete Date	Displays the task's complete date.
Duration	Displays the task's duration.
Repeat Type	Displays the repeat type, for example: non-recurring.
Parent Task	Displays the parent task.
Approval Information	
Approver(s)	Displays a list of task approvers.
Approval Status	Displays the task approval status.
Priority	Displays the task priority.

Field	Description/Action
Approved By	Displays the date and time the task must be approved.
New Comments	Enter additional comments about the task.
Approve Button	Click the Approve button to approve the task.
View Task Details link	Clicking the View Tasks link opens the Diagnostics History page.
Additional Information	
Result Details	Displays the diagnostics that were automatically run (depending on the device type), for example: • Diagnostic “NA Module Status” completed • Diagnostic “NA Routing Table” completed • Diagnostic “NA Interfaces” completed • Diagnostic “NA OSPF Neighbors” completed
Task History	
Task History Information	Displays task history information, such as when the task was run, the repeat type, and status.

Viewing Task Load

The Task Load page provides a glimpse into the health of the NA task subsystem. This page includes all running and waiting tasks, including tasks the current user might not have permission to view.

In a single NA core environment, the Task Load page displays information about the tasks on the NA core.

In a Horizontal Scalability environment, the Task Load page displays information about the tasks on each NA core in the environment.

The Task Load page refreshes automatically.

To view the Task Load page, on the menu bar under Tasks, click Task Load. The Task Load page opens. (You can also access this page under Admin.)

Task Load Page

Field	Description
Local Core Information In a single NA core environment, this table displays information about the tasks on the NA core. In a Horizontal Scalability environment, the Local Core table displays information about the tasks on the NA core to which the NA console is connected.	
Max Concurrent Tasks	The current configuration for the Max Concurrent Tasks setting. To adjust this value, click the Max Concurrent Tasks link.
Tasks Running	The number of currently running tasks. If this value is less than the value of the Max Concurrent Tasks setting, see the Message field for an explanation of the difference.
Tasks Waiting	The number of tasks waiting to be run. As each running task completes, NA starts one of the waiting tasks.
Message	A statement that answers the following question: How does the number of running tasks compare to the Max Concurrent Tasks setting?
Efficiency	A brief description of how well NA is processing the current task load. Possible values are: • Optimal • Moderate • Poor For information about tuning NA to process tasks more efficiently, see the *NA Administration Guide*.
Remote Core Information In a Horizontal Scalability environment, the Remote Cores table displays information about the tasks on the other NA scores.	
Name	The name of the NA core.
Core Hostname	The hostname of the NA server.

Field	Description
Tasks Running	The number of tasks currently running on the core.
Tasks Waiting	The number of tasks waiting to be run on the core.

Chapter 8: Managing Policy Assurance

Use the following table to quickly locate information.

Topic	**Refer to:**
Getting Started	"Getting Started" on page 414
Creating a Policy	"Creating a Policy" on page 416
Creating a Policy Rule	"New Rule Page Fields" on page 422
Importing/Exporting Policies	"Importing/Exporting Policies" on page 426
Editing a Policy	"Editing a Policy" on page 427
Viewing Applied Policies	"Viewing Applied Policies" on page 431
Viewing Policy Activity	"Viewing Policy Activity" on page 432
Viewing Policy Compliance	"Viewing Policy Compliance" on page 433
Adding a New Compliance	"Adding New Software Levels" on page 435
Testing Policy Compliance	"Testing Policy Compliance" on page 441

Getting Started

The HP Network Automation (NA) Policy Manager enables you to establish standards, or best practices, to ensure your network meets your security, reliability, and quality goals. By providing policy enforcement capability and integrated remediation, NA automates the laborious task of validating that devices and configurations match defined best practices, as well as the remediation steps required to bring the device back into compliance with those best practices.

The NA Policy Manager also plays a critical role in meeting regulatory compliance requirements, such as PCI or Sarbanes-Oxley (SOX) in a cost-effective and efficient manner.

The following terms are used in this section:

- Policy — A Policy is a collection of rules that test the configuration and run-time state of your devices.
- Rule — A Rule is an automated test that validates at least one of the following:
  - Specific configuration settings
  - Specific data model element
  - The run-time state of a device (also known as a Diagnostic)
  - The software version running on a device
- Diagnostic — A Diagnostic is a command that is run on a device to collect information about the device that is not captured in its configuration file. For example, on a Cisco router, a Diagnostic would be the output of the command Show NTP Status. Refer to the Diagnostics field in the "View Menu Options" on page 203 section for a list of Diagnostics.
- Rule Exception — A rule exception is part of a rule. However, its purpose is to exclude text it matches in the device configuration from consideration by the rule it is part of.
- Auto-remediation — A pre-defined script that will run automatically when a device is out of compliance with a policy rule.

How the NA Policy Manager Works

To get started with the NA Policy Manager, you first create policies within NA to define the best practice standards to which devices must adhere. Next, you test your policies to validate that they are correctly catching violations. Finally, you assign each policy to a specific device group (or a set of device groups). As a result, NA automatically validates that devices match the defined policies.

Each time a device changes, e.g., the device is reloaded or experiences a configuration change, NA validates that device against the policy assigned to its device group. If the device fails the Policy check, the device is marked as out of compliance. If a change to a device (or group of devices) is non-compliant, the NA Policy Manager generates an event and triggers a notification rule. As a result, you can correct the non-compliant change, preserving both compliance and network availability.

You can summarize the policy compliance status for all of your managed devices. This enables you to provide a risk-rated snapshot of your policy compliance statuses and quickly identify and resolve high-risk configuration and software level violations.

When NA runs a policy check against a device, it processes each rule and checks whether the rule applies to the device or not. If the rule applies, the device is tested against the rule. If the rule does not apply, the rule is skipped for that device.

Rules can be applied in two ways:

- The rule is device family specific. The rule is only checked against a device if the device is using a specific driver, such as Cisco IOS or Juniper JunOS. For example, if you create a rule to apply to devices with Cisco IOS drivers, the rule is never validated against an Extreme switch.
- The rule is device family indifferent. The rule is validating criteria in the normalized data model and therefore is not device family specific. By default, NA parses configuration and device information into normalized elements for its data model. This includes device attributes, such as model number, hostname, location, and so on. Because this data is normalized across all device families, it is not device family specific. As a result, you can apply the rule to all device families, thereby eliminating the need to create a specific rule for each device family in your network.

Note: If you set a rule to all device families, you should not use the config or config block criteria in that rule. Config and Config Block formats are device family specific. If you use the config or config block criteria and set the rule to support all device families, you will get numerous false positives, as NA attempts to find the configuration text in each device configuration.

When executing a policy that checks configuration text, NA removes any leading white spaces by default. As a result, when defining a configuration text that could have leading white spaces, be sure to formulate the regular expression such that it will look for the white space character(s).

For example, if the configuration text on which to search is (note that there are two leading white spaces at beginning of the line):

```
  description this yields unexpected results
```

you would typically use the following regular expression to define the configuration text block that the policy should look for:

```
\s+description.*
```

Note: `\s` is the regular expression that matches any white space character. When you run the policy against the configuration, however, the configuration fails the policy. When the `\s` is removed from the configuration text definition in the policy rule, the configuration passes the policy because NA strips off the leading white spaces by default from the configuration text.

Creating a Policy

Before you can create policies rules, you need to create a policy. To create a policy, on the menu bar under Policies click Policy List. The Policies page opens.

NA ships with several default policies, including the NSA Router Best Practices policy. Some examples of policies you might want to configure include:

- All configurations in a device group must have Access List 110 defined.
- All Fast Ethernet interfaces must have duplex set to Auto Negotiate.
- All border routers must have certain DNS servers.

Note: You can navigate directly to the New Policy page by clicking the New policy option, or you can view the existing polices on the Policies page and then click the New Policy link at the top of the page.

Policies Page Fields

Field	Description
New Policy link	Opens the New Policy page, where you can create a new configuration policy. Refer to "New Policy Page Fields" on page 419 for information.
Check Policy Compliance link	Opens the Check Policy Compliance task page, where you can check for policy compliance. Refer to "Check Policy Compliance Task Page Fields" on page 374 for information. (**Note**: You can also navigate to the Check Policy Compliance task page by clicking the Check Policy Compliance option under Policies --> Policy Tasks on the menu bar.)
Import/Export link	Opens the Import/Export Policies page, where you can import a pre-configured configuration policy or export a configuration policy to a file. Refer to "Importing/ Exporting Policies" on page 426 for information. (**Note**: You can also navigate to the Import/Export Policies page by clicking the Import/Export Policies option.)
Policy Tag drop down menu	Enables you to select a policy tag. As a result, you can easily group policies.
Check Boxes	You can use the left-side check boxes to manage configuration policies. Once you have selected the policies, click the Actions drop-down menu and click either: • Activate — Instructs NA to check the compliance configurations against the selected policies. • Deactivate — Instructs NA not to check the compliance configurations against the selected policies. • Batch Edit — Enables you to batch edit policies. As a result, you can easily change the policy status (Active or Inactive) and the device groups (i.e., Scope) to which the policies are applied. • Delete — Deletes the selected polices. The adjacent Select drop-down menu enables you to select or deselect all of the polices.
Policy Name	Displays the policy name.
Status	Displays the policy's status, either Active or Inactive.
Partition	If you have created Partitions for security or business reasons, you can partition polices for a specific Partition. Keep in mind that you can configure polices to be shared by all users in a Partition, as well as for specific users in specific Partitions. If the policy is available to all Partitions, it is labeled [Shared]. Refer to "Segmenting Devices and Users" on page 150 for detailed information on creating Partitions.
CVE	Displays the CVE (Common Vulnerabilities and Exposures) name. CVE is a list of standardized names for vulnerabilities and other information on security exposures.
Create Date	Displays the date the policy was created.

Field	Description
Actions	You can select the following action: • View & Edit — Opens the Edit Policy page, where you can edit the configuration policy. Refer to "Editing a Policy" on page 427 for information. • Test — Opens the Test Policy Page, where you can test policies against a device or group of devices. (**Note**: Because determining if a policy includes a rule causes performance issues, the Test option is displayed next to each policy, regardless of if it's testable or not. Refer to "Test Policy Page Fields" on page 441 for information.)

New Policy Page Fields

To open the New Policy page, on the menu bar under Polices, click New Policy. The New Policy page opens.

Field	Description/Action
New Policy	
Policy Name	Enter the policy name. A policy is a set of rules applied to a device or a group of devices.
Policy Description	Enter a description of the policy.
Partition	Select a Partition from the drop-down menu. (**Note**: This field is only displayed if you have configured one or more Partitions.) In general, a Partition is a grouping of devices with unique IP addresses. Multiple Partitions can be managed by a single NA Core. A NA Core is an installation of a NA server, comprised of a single Management Engine, associated services, and a single database. Refer to "Segmenting Devices and Users" on page 150 for detailed information on creating Partitions.
Policy Tag	Select one of the following options: • General purpose — If you do not want to tag a policy, it is used as a general purpose policy. • Existing — Select a tag from the drop-down menu. • New — Create a new policy tag by entering a tag name.
Scope	Select one of the following options: • Select the device groups to which this policy applies — Use the Device Selector to select groups. For information on how to use the Device Selector, refer to "Device Selector" on page 144. • Use filters to define a dynamic policy scope — A policy scope includes the devices a policy can potentially affect. Keep in mind that the policy scope can only affect a given device if the policy has a policy rule that affects the device family containing the device. When defining a policy, you can define the policy scope the same way you define a Dynamic Group. As a result, you can create a private Dynamic Group in conjunction with a policy. (Refer to "Dynamic Device Groups" on page 142 for information on creating Dynamic Groups.)
Search Criteria (when using filters to define a dynamic policy scope) Each time you select a search criterion from the Add Criteria drop-down menu, it is displayed in the Search Criteria section, where you can then select an operator, such as Contains, Matches, or Equals, and enter the information on which to search. If you want to delete a defined criterion, click the X next to the search criterion index letter.	
Add Criteria	Select one or more search criteria from the drop-down menu, for example: • Configuration Text • Device IP • Device Status • Host Name • Password Rule

Field	Description/Action
Boolean Expression	
Expression	By default, the defined criteria index letters are displayed with the Boolean ‘and’ expression. For example, if you defined three search criteria, the expression would look like *A and B and C*. You can edit the Boolean expression as needed. Click the Reset Expression button to reset the expression to the default. (**Note**: The Boolean operator must be entered in lowercase. In addition, the maximum number of criteria is 10.)
Limit search by device group	
Device belongs to	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use Shift+click to select/deselect multiple device groups. If you do not select a device group, NA will discard the device group filter when searching.
Limit search by view and partitions (This information is displayed if you have configured Views and Partitions. Refer to “Segmenting Devices and Users” on page 150 for information.)	
..but not these devices	Enter the IP address or hostname of the device in the right-hand box and then click Add Exception <<. To remove a device, select the IP address or hostname of the device in the left-hand box and click Remove Exception.
Policy Rules	The Policy Rules table displays all rules that will be applied by the policy. The policy applies all rules to each saved device selected for this policy. Keep in mind that rules are applied in no particular order.
New Rule button	To create a new rule for this policy, click the New Rule button. The New Rule page opens. Refer to “New Rule Page Fields” on page 422 for information.
Detailed Description	Enter a detailed description of the policy. Keep in mind that a short description of the policy appears in any list in which the policy appears. This field enables you to add a detailed description of the policy.
Policy Status	Click one of the following options: • Active — Marks the policy active (the default). • Inactive — Deactivates the policy.
Additional Policy Fields (These fields are automatically populated when the policy is from The HP Security and Compliance Service.)	
CVE	Enter the CVE (Common Vulnerabilities and Exposures) name. CVE is a list of standardized names for vulnerabilities and other information on security exposures. (For more information, refer to www.cve.mitre.org.)
Vendor Advisory URL	Enter the URL to an external reference for advisory information on a vulnerability. Keep in mind that when creating a policy and including a vendor advisory URL and/or a vendor solution URL, the URL must start with the “http://” prefix, otherwise the link might not be correctly interpreted by the browser. Note that if the URL field is left blank, when selected, the link could open the NA home page.

Field	Description/Action
Vendor Solution URL	Enter a URL to an external reference for more information on possible solutions to the vulnerability.
Disclosure Date	Enter the date when the software vulnerability was flagged in the following format: *yyyy-MM-dd*.
Solution	Enter detailed solution information.

Be sure to click the Save button when you are finished.

New Rule Page Fields

When you click the New Rule button on the New Policy page, the New Rule page opens. Keep in mind that rules can be applied in two ways:

- The rule is device family specific. The rule is only checked against a device if the device is using a specific driver, such as Cisco IOS or Juniper JunOS. For example, if you create a rule to apply to devices with Cisco IOS drivers, the rule is never validated against an Extreme switch.
- The rule is device family indifferent. The rule is validating criteria in the normalized data model and therefore is not device family specific. By default, NA parses configuration and device information into normalized elements for its data model. This includes device attributes, such as model number, hostname, location, and so on. Because this data is normalized across all device families, it is not device family specific. As a result, you can apply the rule to all device families, thereby eliminating the need to create a specific rule for each device family in your network.

Field	Description/Action
New Rule	
Rule Name	Enter the rule name.
Rule Type	Select a rule type. For example, you can define a rule based on the configuration text or data model elements pulled from configuration text of the selected device(s). Options include: • Configuration — If selected, the configuration rule checks to see if the selected device(s) configuration text is in compliance with the current configuration rule. • Diagnostics — If selected, the rule checks to see if the selected device(s) Diagnostic text is in compliance with current Diagnostic rule. Diagnostic text is generated by running diagnostics. Refer to “Run Diagnostics Task Page Fields” on page 312 for information. (**Note**: Use caution when renaming diagnostics on which policy rules are based. If you rename the diagnostic on which a policy rule is based, you will lose the policy rules condition. • Software — If selected, the rule checks to see if the selected device(s) are in compliance with the current software rule. Refer to “Software Level Report Fields” on page 620 for information.
Rule Description	Enter a description of the rule.
Applies to devices with these drivers	
All Device Families	Click the radio button if you want to apply the rule to all device families. By default, NA parses configuration and device information into normalized elements for its data model. This includes device attributes, such as model number, hostname, location, and so on. Because this data is normalized across all device families, it is not device family specific. **Note:** If you set a rule to all device families, you should not use the config or config block criteria in that rule. Config and Config Block formats are device family specific. If you use the config or config block criteria and set the rule to support all device families, you will get numerous false positives, as NA attempts to find the configuration text in each device configuration.

Field	Description/Action
Device Family	Select the device family to which the rule applies from the drop-down menu, for example BayStack, Cisco IOS or Nortel ASF. Select one of the following options: • All applicable drivers — If checked (the default), NA chooses all applicable drivers. Keep in mind that a rule applies only to devices that are assigned a specific driver. • Select specific drivers — If checked, select one or more drivers from the list. Keep in mind that a configuration rule applies only to the configuration for devices that are assigned a specific driver.
Define Text Block	Enables you to set text blocks to be used by configuration block conditions. If you select the Set Text Blocks option, the Block Start Pattern and the Block End Pattern fields are displayed. These are only used if a condition of the type “Config Block” is added. The condition is applied to specific blocks of text within the configuration file, such as a single interface in a Cisco IOS device. If you are applying the rule to each instance of a specific block within the configuration file, enter the block start pattern, for example *interface .** and the block end pattern, for example *!*.
Define Text Block (*continued*)	The configuration text extracted by the block start and end patterns includes the lines that match the start and end patterns. As a result, any Config Block condition will be matched against not only the lines between the start and end patterns, but also the lines that match the start and end patterns. For example, if you have the following block start and end patterns:

```
block start: interface .*
block end : !
```

And the configuration text includes the following lines:

```
...
no service pad
service timestamps log uptime
service timestamps log uptime
interface FastEthernet0/7
description testfor bug 145762
speed 100
duplex full
!
ip default-gateway 10.255.1.1
ip http server
...
```

The extracted portion of the configuration to be used for any Config Block condition matches will be:

```
interface FastEthernet0/7
description testfor bug 145762
speed 100
duplex full
!
```

Note that it includes lines that match with the start and end patterns, `interface FastEthernet0/7` and `!` respectively.

Field	Description/Action
Rule Conditions	Select one or more conditions from the drop-down menu, for example Config Text, Flash Memory, and Host Name. • Regular Expression — When checked, the pattern is a regular expression. When not checked, the pattern is a string to be matched against the configuration (diagnostics) text or the data model element value. • Must contain — Configuration (diagnostics) text or the value of the data model element must contain the pattern. • Must not contain — Configuration (diagnostics) text or the value of the data model element must not contain the pattern. • Must contain only — Configuration (diagnostics) text or the value of the data model element must contain the pattern, but must not contain any other matches for the pattern given in “But must not have any additional lines containing:” field. • Lines in Exact Order — When checked, pattern lines must match in the given sequence. Each line in a condition pattern is interpreted as an independent pattern and checked separately. When this option is checked, those independent matches must be in the given sequence without any unmatched characters (other than white space). In addition to using “and” and “or” to build a Boolean expression, you can configure conditional rules using “if-then-else” logic, in which “else” is optional. For example, if you define five conditions from ‘A’ to ‘E’, the Boolean expression could be built as: *“if (A and B) then (C or D) else E”*. (**Note**: The Boolean operator must be entered in lowercase. In addition, the maximum number of criteria is 10.) The get help link provides information on using regular expressions. The Device Variables link opens the Device Variables page. The page includes a list of built-in variables you can use in your Policy Rule definition. As a result, their values are replaced when the Policy Rule is being checked. Click the Reset Expression button to reset the expression to the default.
Importance	Select the importance level. This indicates the non-compliance risk rating for the policy rule. NA can sort violations based on their severity. For example, Critical violations can automatically open a trouble ticket in the Change Management system, while Informational violations can be identified in a daily report. Options include: • Informational — Events that typically do not require a response. • Low — Events that may require a response as time permits. • Medium — Events that require a timely response, typically within 72 hours (the default). • High — Events that require an urgent response, typically within 24 hours. • Critical — Events that require an immediate response.
Detailed Description	Enter a description of the rule.
Rule Exceptions	Displays a list of rule exceptions, if applicable. A rule exception is part of a rule. For example, a rule exception can exclude text it matches in the device configuration from consideration by the configuration rule it is part of. To add an Exception Rule, click the New Exception link. The New Rule Exception page opens. (Refer to “Adding a Rule Exception” on page 430 for information.)

Field	Description/Action
Auto-Remediation Scripts	The Auto-remediation pop-up window accesses the data on the Policy Rule page to show variable mappings, generate sample code, and validate the script before it is saved. An Auto-remediation script enables you to define variables in the script that reference data from regular expression pattern groups in a violated policy rule. (Refer to "Creating Auto-remediation Scripts" on page 587 for more information.) To add a new Auto-remediation script, click the New Auto-Remediation Script link. The Auto-remediation script pop-up window includes a command script page. To assist in entering Auto-remediation scripts, you can select the following links: • Show Variables — Displays the variable mappings in regular expression patterns. This enables you to view what portions of the patterns apply to which regular expression groups. The highlighted portions on the regular expression pattern are referenced with the variable on the left. Note that the section before the (.*) in the variable must be replaced with the `@foreach` loop variable. The variable names show regular expression groups. In addition, the regular expression group 0 (zero) represents the entire pattern. • Generate Sample Code — Generates sample template code with variables that you can use. Device commands must be added into `@foreach` loops. Device commands can reference the variables listed in each generated loop above.

When you are finished, you can either click the Save button to save the rule, the Save And Add Another button to save the current rule and add a new one, or the New Exception link to add a new rule exception.

Importing/Exporting Policies

You can import pre-defined policies or export policies to a file. This enables you to easily share policies.

Note: When importing policies that were exported from a different NA application server, determine the names of all diagnostics referenced by the imported policies. Diagnostics of the same name and function system must exist on the target system.

To import or export a policy, on the menu bar under Policies, click Import/Export Policies. The Import/Export Policies page opens.

To print a policy, on the Import/Export Policies page, select that policy in the Export Policy area, and then click **Print**. On the results page, use the web browser functionality to print the output, and then use the web browser's back functionality to return to the NA console.

Note: NA is able to import policies of previous versions, starting with NA 6.2.

Import/Export Policies Page Fields

Field	Description/Action
Import Policy	Enter the policy file to import or click the Browse button to locate the policy file. When the policy file is displayed, click the Import button. If a policy already exists, you are prompted to rename it.
Export Policy	Displays a list of the current configuration policies. Click the configuration policies you want to export and then click the Export button. Keep in mind that the device groups associated with the configuration policy are not exported. Also, any configuration policy exception rules are not exported.

Editing a Policy

To edit a policy:

1. On the menu bar under Policies, click Policy List. The Policies page opens.
2. Click the View & Edit action for the policy you want to edit. The Edit Policy page opens. Be sure to click Save when finished.

Edit Policy Page Fields

Field	Description/Action
Policy Name	Displays the policy name.
Policy Description	Displays a description of the policy.
Partition	Select a Partition from the drop-down menu. (**Note**: This field is only displayed if you have configured one or more Partitions.) In general, a Partition is a grouping of devices with unique IP addresses. Multiple Partitions can be managed by a single NA Core. A NA Core is an installation of a NA server, comprised of a single Management Engine, associated services, and a single database. Refer to "Segmenting Devices and Users" on page 150 for detailed information on creating Partitions.
Policy Tag	Select one of the following options: • General purpose — If you do not want to tag a policy, it is used as a general purpose policy. • Existing — Select a new policy from the drop-down menu. • New — Enter the location of the policy.
Scope	Select one of the following options: • Select the device groups to which this policy applies — Select one or more device groups from the list. You can use Shift+click or Ctrl+click to select multiple device groups. • Use filters to define a dynamic policy scope — A policy scope includes the devices a policy can potentially affect. Keep in mind that the policy scope can only affect a given device if the policy has a policy rule that affects the device family containing the device. When defining a policy, you can define the policy scope the same way you define a Dynamic Group. As a result, you can create a private Dynamic Group in conjunction with a policy. (Refer to "Dynamic Device Groups" on page 142 for information on creating Dynamic Groups.)

Field	Description/Action
Search Criteria (when using filters to define a dynamic policy scope) Each time you select a search criterion from the Add Criteria drop-down menu, it is displayed in the Search Criteria section, where you can then select an operator, such as Contains, Matches, or Equals, and enter the information on which to search. If you want to delete a defined criterion, click the X next to the search criterion index letter.	
Add Criteria	Select one or more search criteria from the drop-down menu, for example: • Configuration Text • Device IP • Device Status • Password Rule • Host Name
Boolean Expression	
Expression	By default, the defined criteria index letters are displayed with the Boolean ‘and’ expression. For example, if you defined three search criteria, the expression would look like *A and B and C*. You can edit the Boolean expression as needed. Click the Reset Expression button to reset the expression to the default. (**Note**: The Boolean operator must be entered in lowercase. In addition, the maximum number of criteria is 10.)
Limit search by device group	
Device belongs to	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use Shift+click to select/deselect multiple device groups. If you do not select a device group, NA will discard the device group filter when searching.
Limit search by view and partitions (This information is displayed if you have configured Views and Partitions. Refer to “Segmenting Devices and Users” on page 150 for information.)	
..but not these devices	To add an IP address or hostname of the device, enter the Host name or IP address in the right-hand box and then click Add Exception <<. To remove a device, select the IP address or hostname of the device in the left-hand box and click Remove Exception.
Policy Rules	Displays all rules that will be applied by the policy. The policy applies all configuration rules to each saved device selected for this policy. Keep in mind that rules are applied in no particular order. The importance column displays either Informational, Low, Medium, High, or Critical. This indicates the non-compliance risk rating for the policy rule. Click the View & Edit link in the Actions column to edit the rule.
New Rule button	To create a new rule for this policy, click the New Rule button. The New Rule page opens. Refer to “New Rule Page Fields” on page 422 for information.
Detailed Description	Displays a detailed description of the policy.

Field	Description/Action
Policy Status	Click one of the following options: • Active — Marks the policy active (the default). • Inactive — Deactivates the policy.
Software Policy Fields (These fields are automatically populated when the policy is from the HP Security and Compliance Service.)	
CVE	Displays the CVE (Common Vulnerabilities and Exposures) name. CVE is a list of standardized names for vulnerabilities and other information on security exposures. (For more information, refer to www.cve.mitre.org.)
Vendor Advisory URL	Displays the URL to an external reference for advisory information on a vulnerability.
Vendor Solution URL	Displays a URL to an external reference for more information on possible solutions to the vulnerability.
Disclosure Date	Displays the date when the software vulnerability was flagged in the following format: *yyyy-MM-dd*.
Solution	Displays detailed solution information.

Adding a Rule Exception

A rule exception is part of a rule. Like a rule, it is a regular expression. However, its purpose is to exclude text it matches in the device configuration from consideration by the configuration rule it is part of.

An exception rule typically excludes either a text pattern or a specific device configuration from the configuration rule. Exceptions are usually created when one or more device configurations do not comply with a rule, but you cannot alter the rule to fit all similar configurations.

To add a rule exception to an existing configuration rule:

1. On the menu bar under Policies, click Policy List. The Policies page opens.
2. Select the policy to which you want to add the exception and click View & Edit. The Edit Policy page opens.
3. Find the rule inside the policy that needs an exception and click View & Edit. The New Rule page opens.
4. Click the New Exception link at the bottom of the page. The New Rule Exception page opens.

New Rule Exception Page Fields

Field	Description/Action
Device	Enter the IP address or hostname of the device to which this exception rule applies.
Expires on	If checked, choose the month, day, year, hour, and minute after which this exception is disregarded by the rule. An exception rule’s expiration date is the date after which the exception ceases to have any effect on the rule it is part of. Although the exception rule continues to exist after its expiration date, the configuration policy applies the rule as if the exception rule does not exist.
Ignore text matching this pattern when checking the configuration rule	If checked, enter text. All text in a device’s configuration that matches the text you entered is not subject to this configuration rule. (**Note**: The get help link provides examples.)
Ignore this device entirely when checking the configuration rule	If checked, NA skips this device when checking the configuration rule.

Be sure to click the Save button when you are finished.

Viewing Applied Policies

You can view policies that apply to a device. As a result, you can:

- Verify that the correct policy was applied to the device
- View if the policy passed or failed
- View policies that are applied to the device when the device is added to NA
- View the exceptions that are in place for a policy applied to the device

To view applied policies:

1. Create a new policy for a device. Refer to "Creating a Policy" on page 416 for information.
2. Run the policy against the device. Refer to "Policy Compliance Page Fields" on page 433 for information.
3. Open the Device Details page for the device.
4. Click the View menu.
5. Select Device Details and click Polices. The Device Polices Page opens. Refer to "Device Policies Page Fields" on page 223 for information.

Viewing Policy Activity

You can view events that show a device's configuration was not in compliance with the rules contained in one or more policies. The events indicate when NA detected and recorded that a device was non-compliant.

To view the Policy Activity page, on the menu bar under Policies, click Policy Activity. The Policy Activity page opens.

Policy Activity Page Fields

Field	Description/Action
For the (time frame)	Select the time frame in which you want to view non-compliance events. The default is the past hour.
Current Working Group	Select the group for which you want to view non-compliance events. The default is Inventory, which includes all other groups.
Event Date	Displays the date the policy was found to be in non-compliance.
Policy Name	Displays the name of the policy. Click this link to open the Edit Policy page. You can edit the policy and any included rules. Refer to "Editing a Policy" on page 427 for information.
Host Name	Displays the host name of the device. Click this link to view basic information about the device.
Device IP	Displays the IP address of the device. Click this link to view basic information about the device and its configuration history.
Summary	Displays the event type (Configuration Policy Non-Compliance). Click this link to open the System Event Detail page, where you can view details of the non-compliance event.
Importance	Indicates the importance of the rule that was violated, including: • Informational — Events that typically do not require a response. • Low — Events that may require a response as time permits. • Medium — Events that require a timely response, typically within 72 hours. • High — Events that require an urgent response, typically within 24 hours. • Critical — Events that require an immediate response.

Viewing Policy Compliance

The Policy Compliance page enables you to view the devices whose configurations are or are not in compliance with configuration policies.

To view the Policy Compliance page, on the menu bar under Policies, click Policy Compliance. The Policy Compliance page opens.

Policy Compliance Page Fields

Field	Description/Action
Check Policy Compliance link	Opens the Check Policy Compliance task page, where you can check for configuration compliance. Refer to "Check Policy Compliance Task Page Fields" on page 374 for information.
Current Working Group	Select the group for which you want to view device compliance status.
Display only devices that are not in compliance	If checked, devices that are in compliance are not displayed.
Host Name	Displays the host name of the device. Click this link to view basic information about the device.
Device IP	Displays the IP address of the device. Click this link to view basic information about the device and its configuration history.
Policy Compliance	• Yes — Indicates that the device's configuration is in compliance with all polices. • No — Indicates that the device's configuration is not in compliance with all configuration policies. Clicking No opens the Configuration Policy Activity page. Refer to "Policy Activity Page Fields" on page 432 for information. • Unknown — Indicates devices that have not had their policy compliance checked.
Partition	Displays the Partition to which the device belongs, if applicable.
Last Changed Time	Displays the date and time the device's configuration was last changed.
Actions	You can select the following options: • Policy Events — Opens the Configuration Policy Activity page, where you can view the details of the non-compliance event. Refer to "Policy Activity Page Fields" on page 432 for information. • Policies Applied — Opens the Configuration Policies that Apply to Device page, where you can view the configuration polices and rules for a specific device. Refer to "Configuration Policies That Apply to Device Page Fields" on page 434 for information.

Configuration Policies That Apply to Device Page Fields

To view the Configuration Policies That Apply to Device page:

1. On the menu bar under Policies, click Policy Compliance.
2. In the Actions column for the device on which you need information, click the Policies Applied link. The Configuration Policies That Apply to Device page opens.

Field	**Description/Action**
Policy Name	Displays the name of the configuration policy applied to the device.
Rule Name	Displays the name of the configuration rule applied to the device.
Out of compliance key	Displays if the device is currently out of compliance, including: • High Importance (red) • Medium Importance (amber) • Low Importance (green)
Actions	You can select the following options: • Host name or IP address — Opens the Device Information page, where you can view basic information about the device and its configuration history. • Policy Name — Opens the Edit Configuration Policy page, where you can edit the policy and add/edit configuration rules. Refer to “Editing a Policy” on page 427. • Rule Name — Opens the Edit Configuration Rule page, where you can edit the configuration rule. Refer to “Adding a Rule Exception” on page 430.

Adding New Software Levels

As the number of network device security alerts and notifications about security vulnerabilities continue to increase, many organizations are faced with tracking which OS version is present on each device and whether that OS version is vulnerable to security issues. NA enables you to specify OS versions that are susceptible to security problems and then generate alerts or automated responses when those versions are detected. Keep in mind that you can group images into categories, such as “pre-production” or “Obsolete.” Images can also be classified, for example “Security Risk,” based on recently discovered vulnerabilities.

To add a new software level or review existing compliance definitions:

1. On the menu bar under Polices, click Software Levels. The Software Levels page opens. (Refer to “Software Levels Page Fields” on page 437 for information on the Software Levels page.)
2. Click the Add Level link. The Add Level page opens. Be sure to click Save when you are finished.

Add Software Level Page Fields

Field	Description/Action
Add Software Level	
Level Name	Enter the level name.
Status	Displays one of the following options: • Active — Marks the configuration policy active (the default). • Inactive — Deactivates the configuration policy. Inactive policies do not generate non-compliance events.
Level	Select a compliance rating name. You can use any of the compliance definitions given depending on your requirements and validation procedures. Options include: • Security Risk • Pre-production • Obsolete • Bronze • Silver • Gold • Platinum
Description	Enter a description of the compliance. To improve awareness of security issues, any security risk description should include a short title of the vulnerability, any applicable CVE/CAN or CERT designations, and a link to the vendor notice, if available.

Field	**Description/Action**
Partition	Select a Partition from the drop-down menu. If you have created Partitions for security or business reasons, you can partition software levels for a specific Partition. Keep in mind that you can configure polices to be shared by all users in a Partition, as well as for specific users in specific Partitions. If the software level is available to all Partitions, it is labeled [Shared].
Matching Criteria (Matching criteria can use wildcard operators: * and ?.)	
Software Version	Enter the software version for which this compliance policy applies.
Device Driver	Select a device driver used to access the device from the drop-down menu. (Any is the default.)
Device Model	Enter the device model.
Filename	Enter the filename, if applicable.
Configuration Contains	Enter a pattern to match against the current device configuration to determine if the compliance applies to a given device.
Software Vulnerability Information (for Security Risk level)	
Disclosure Date	Enter the date when the software vulnerability was flagged in the following format: *yyyy-MM-dd*.
Importance	Select the severity of the security vulnerability from the drop-down menu, including: • Informational • Low • Medium • High • Critical
CVE Name	Enter the CVE (Common Vulnerabilities and Exposures) name. CVE is a list of standardized names for vulnerabilities and other information on security exposures. (For more information, refer to www.cve.mitre.org.)
Solution	Enter solution information.
Advisory URL	Enter the URL to an external reference for advisory information on a vulnerability.
Solution URL	Enter a URL to an external reference for more information on possible solutions to the vulnerability.

Software Levels Page Fields

NA has the ability to define software levels, essentially a regex to match against software versions. You can assign a software level to that regex. Any device with a software version that matches the regex is considered at that level.

Note: Software levels can be partitioned so that only those with the appropriate permissions can view and edit them. Refer to "Partitions" on page 158 for information.

The Software Levels page enables you to review existing software level definitions.

Field	Description/Action
Add Level link	Opens the Add Software Level page, where you can add a software levels. Refer to "Add Software Level Page Fields" on page 435.
Device Software Report link	Opens the Device Software report, where you can view the software version and compliance rating currently assigned to each device. Refer to "Device Software Report Fields" on page 618.
Software Level Report link	Opens the Software Level report, where you can view the software level currently assigned to each device. Refer to "Software Level Report Fields" on page 620.
View	Select either "User-define policies" or "Security Alert Service alerts" from the drop-down menu. Security Alert Service alerts are events originating from the Security Alert Service. (**Note**: The Security Alert Service is a subscription-based service.)
Check boxes	You can use the left-side check boxes to manage software level definitions. Once you have selected the compliance definitions, click the Actions drop-down menu and click either: • Activate — Instructs NA to activate the software level definition. • Deactivate — Instructs NA to deactivate the software level definition. • Delete — Deletes the software level definition. The adjacent Select drop-down menu enables you to select or deselect all of the polices.
Name	Displays compliance's name.
Version	Displays the software version.
Driver	Displays the driver name.
Model	Displays the model designation of the device.
Filename	You can provide a filename (wildcards are allowed), that the system can use to determine compliance. For example, you can tag all images that begin with router5*.bin as Obsolete.

Field	Description/Action
Software Level	Displays the compliance rating name. Ratings include: • Security Risk • Pre-production • Obsolete • Bronze • Silver • Gold • Platinum
Importance	Displays either Informational, Low, Medium, High, or Critical. This indicates the importance of the compliance rule that was violated. • Informational — Events that typically do not require a response. • Low — Events that may require a response as time permits. • Medium — Events that require a timely response, typically within 72 hours. • High — Events that require an urgent response, typically within 24 hours. • Critical — Events that require an immediate response.
Last Modified	Displays when the software level was last modified.
Partition	If you have created Partitions for security or business reasons, you can partition software levels for a specific Partition. Keep in mind that you can configure software levels to be shared by all users in a Partition, as well as for specific users in specific Partitions. Refer to "Segmenting Devices and Users" on page 150 for detailed information on creating Partitions.
CVE	Displays CVE (Common Vulnerabilities and Exposures) name. CVE is a list of standardized names for vulnerabilities and other information on security exposures.
Comments	Displays a description of the compliance.
Actions	You can select the following options: • Edit — Opens the Edit Compliance page where you can edit the compliance. • Delete — Enables you to delete the compliance.

Editing a Software Level

To edit a software Level:

1. On the menu bar under Policies, click Software Level. The Software Levels page opens.
2. Click the Edit action for the software level you want to edit. The Edit Software Level page opens. Be sure to click Save when finished.

Edit Software Level Page Fields

Field	Description/Action
Edit Compliance	
Level Name	Displays the policy name.
Status	Displays one of the following options: • Active — Marks the configuration policy active (the default). • Inactive — Deactivates the configuration policy. Inactive policies do not generate non-compliance events.
Level	Displays the software level rating name. You can use any of the definitions given depending on your requirements and validation procedures. Options include: • Security Risk • Pre-production • Obsolete • Bronze • Silver • Gold • Platinum
Description	Displays a description of the compliance.
Matching Criteria	
Software Version	Displays the software version for which this compliance policy applies.
Device Driver	Displays the device driver used to access the device.
Device Model	Displays the device model.
Configuration Contains	Displays the pattern used to match against the current device configuration to determine if the compliance policy applies to a given device.
Software Vulnerability Information (for Security Risk compliance level)	
Discloser Date	Displays the date when the software vulnerability was flagged.

Field	Description/Action
Importance	Displays the severity of the security vulnerability, including: • Informational • Low • Medium • High • Critical
CVE Name	Displays the CVE (Common Vulnerabilities and Exposures) name. CVE is a list of standardized names for vulnerabilities and other information on security exposures. (For more information, refer to www.cve.mitre.org.)
Solution	Displays solution information.
Vendor Advisory Link	Displays a URL to an external reference for advisory information on a vulnerability.
Vendor Solution Link	Displays a URL to an external reference for more information on possible solutions to the vulnerability.

Testing Policy Compliance

You can test device configurations for compliance against one or more configuration policies or test your configuration policies against one or more configurations. This enables you to test a device's configuration compliance or test a configuration policy before deployment.

On the menu bar under Policies click Test Policy Compliance. The Test Policy Compliance page opens.

Test Policy Compliance Page Fields

Field	**Description/Action**
Policy List link	Opens the Polices page, where you can view a list of your policies. Refer to "Policies Page Fields" on page 417 for information.
Select the policies to be applied	You can select one of the following options: • All Policies — If checked (the default) all of your configuration policies are tested. • Polices that are applicable to selected device groups — Select a device group for which to run the test against. To select multiple device groups, press the Shift key while selecting device groups. • Selected policies — Select a specific policy. To select multiple policies, press the Shift key while selecting policies.
Test policy against existing devices	Select the devices on which to test the policy against. For information on how to use the Device Selector, refer to "Device Selector" on page 144.
Test policy against configuration	If you select this option, enter or paste the configuration text in the box and select the device family for the configuration text you entered from the drop-down menu.

When you are finished, click Perform Test. If the configuration policy check passes, the "Device [device name] is in compliance with selected and applicable policies" message is displayed in a new window. If the configuration policy check fails, a list of each violation is displayed in the new window with links to detailed information.

Test Policy Page Fields

When you first create a policy, you will want to test the policy to validate that it is correctly catching issues with a device. You may not, however, want NA to generate non-compliance events because that could trigger alerts in your fault management system or upset your network compliance metrics. In this case, using the Test Policy capability is ideal. When you use the Test Policy condition, no events are generated. As a result, you can test the policy without generating any non-compliance events.

When you have selected the devices, click the Perform Test button.

Field	Description/Action
Select the policies to be tested	Select a policy from the drop-down menu.
Select the devices to test against	Select the devices for which to test the policy against. For information on how to use the Device Selector, refer to "Device Selector" on page 144.

Chapter 9: Deploying Software

Use the following table to quickly locate information.

Topic	Refer to:
Getting Started	“Getting Started” on page 444
Software Images	“Software Images” on page 446
Adding Image Sets	“Adding Image Sets” on page 447
Deploying Software	“Deploying Software” on page 450
Adding a New Compliance	“Adding a New Software Level” on page 451
Viewing Device Software Versions	“Viewing Device Software Versions” on page 453

Getting Started

HP Network Automation (NA) provides a central repository of device software, including operating system (OS) images, that you can deploy to one or more devices that share the same software. Having a central storage location guarantees that the last known good software is available in-house.

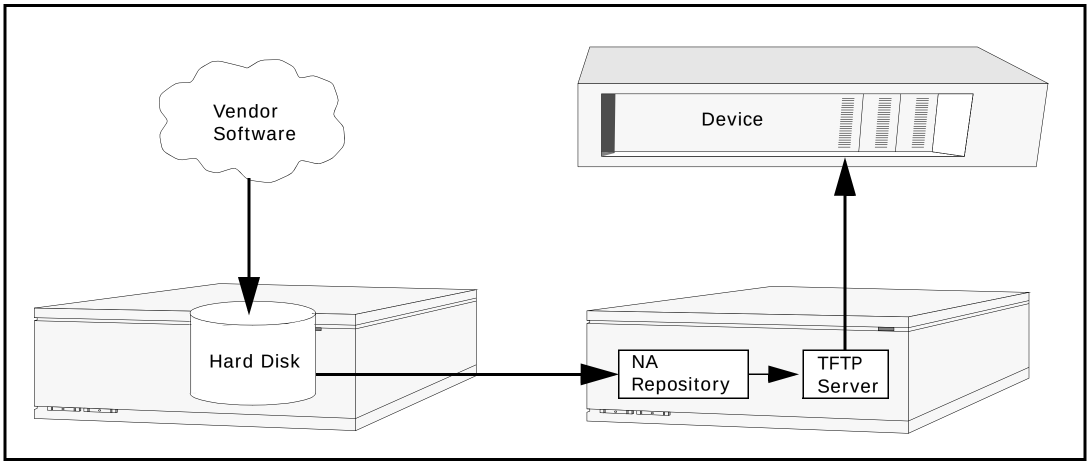
You can:

- Upload software image sets into the system. An image set is a grouping of images that can be deployed to a device simultaneously. An image set can contain one or more images. When you initiate a software upload, you select an image set to be uploaded. Each image in the image set is uploaded in turn. If the device has a problem (e.g. out of memory), the rest of the upload is aborted.
- Add or upload files to a device.
- Define the minimum requirements for an image set, such as the device family, device model, minimum RAM, processor, or boot ROM version required to run the image successfully.
- Prepare a device prior to deploying an image by deleting files to free up flash memory space, and/or compacting the flash memory.
- Reboot a device after deploying an image.
- Schedule updates through NA. For example, you might deploy a new image to one device successfully during the day shift, then schedule updates to many more devices during off-peak hours.
- Define multiple compliance ratings to identify software versions and upgrade devices as resources permit.
- Designate which image should be the Boot image for devices that have multiple Boot images. You can select a Boot image, and if necessary an OS image, currently on the device, or transfer a new Boot and/or OS image. If you select a single Boot and/or OS image, commands are issued on the device to set those images as the images to use for Boot and/or OS. Depending on the device, these will not take affect until the next time the device reboots, which can be selected as part of the Update Device Software task. Refer to "Update Device Software Task Page Fields" on page 325 for information.

Another feature is the Image Synchronization Report, which enables you to view the currently running or backup software images on a device, or group of devices, that do not reside in the NA software image respository. Refer to the "Image Synchronization Report Fields" on page 624 for information.

Note: A Boot image contains the complete contents and structure of system's storage media. The Boot image enables the associated hardware to boot. An OS image contains instructions for running a device after the device is on and has gathered information regarding its interfaces. The OS image contains items such as routing protocols.

The figure below illustrates the download process.



There are several best practices that you should follow when using the software update feature. HP recommends the following practices when deploying software images:

- Follow your standard change control and approval processes. Any time you modify the state of a device some risk is entailed. To minimize the impact this could have on your network, adhere to all defined change processes in the organization, such as approvals, notifications, change windows, and so on.
- Research and understand the proper steps for updating a given device and OS version. On some devices, multiple images may be required to upgrade. In addition, there may be firmware or hardware dependencies.
- Test the functionality of a given OS version before deploying it on a production network. When upgrading (or particularly when downgrading) OS versions, the device configuration may be altered or may need to be updated prior to or after the change. Before deploying a given version in production test it thoroughly in a test-lab environment to ensure the configuration upgrades successfully and the device functions as expected.
- Backup your current device images. Use the NA repository to store the existing images on your devices before upgrading them. This way you can quickly recover should a new image exhibit any unexpected results. Keep in mind that the Image Synchronization report enables you to view the currently running or backup software images on a device, or group of devices, that do not reside in the NA software image repository. Refer to the "Image Synchronization Report Fields" on page 624 for information.
- When upgrading a device, it is a good idea to have out-of-band management access to the device via a console server.
- Provide image requirements and verify them carefully. NA enables you to specify the requirements for each software image.
- When deploying images to business critical devices, do not use the auto-reboot function. Rather, use the software update feature to prepare the devices and load the images, then manually inspect each device to be sure it is in a clean state before rebooting it.
- Update a single device first before updating a group of devices.

Software Images

Before you upgrade a device's software, you should be aware of the currently installed software on each device, including:

- Image set
- Filenames
- Required driver

On the menu bar under Devices, select Device Tools and click Software Images. The Software Images Page opens.

Software Images Page Fields

Field	Description/Action
Add Image Set from Cisco.com link	Opens the Download Image From Cisco.com Task page. Refer to "Download Image From Cisco.com Task Page" on page 369 for information.
Add Image Set link	Opens the Add Software Image Set page, where you can add an Image Set. Refer to "Adding Image Sets" on page 447 for information.
Software Levels link	Opens the Software Levels page, where you can add a new software level or view the Device Software report. Refer to "Adding New Software Levels" on page 435 for information on adding a new level. Refer to "Device Software Report" on page 618 for information on the Device Software report.
Image Set	Displays the name of the Image Set.
Driver Required	Displays the name of the NA driver required for this platform.
Model Required	Displays the name of the required model. Note that this field has been expanded from 255 characters to 4,000 characters so as to accommodate all possible models.
Hardware Required	Displays hardware requirements, if applicable.
Partition	If you have created Partitions for security or business reasons, you can partition software images according to Partitions. If the software image is available to all Partitions, the software image is labeled "Shared" (or "Global") depending on configuration. Keep in mind that you cannot edit or delete software images without the proper permissions. Refer to "Segmenting Devices and Users" on page 150 for detailed information on creating Partitions.
Actions	You can select the following options: • Edit — Opens the Edit Software Image page, where you can edit existing software information. Refer to "Edit Software Image Page Fields" on page 449 for information. • Software Images — Opens the Manage Images in Set page, where you can edit the image set, add images, and deploy software. Refer to "Add Software Image Set Page Fields" on page 447, "Edit Software Image Page Fields" on page 449, or "Deploying Software" on page 450. • Delete — Enables you to delete the image. • Update Device — Opens the Update Device Software Task page. Refer to "Deploying Software" on page 450 for information.

Adding Image Sets

To add Image Sets:

1. On the menu bar under Devices, select Device Tools and click Software Images. The Software Images page opens.
2. Click the Add Image Set link. The Add Software Image Set page opens. Be sure to click the Save Software button when finished.

Note: The file size cannot be larger than 256MB.

Add Software Image Set Page Fields

Field	Description/Action
Image Set Name	Enter the Image Set Name. All images in a particular Image Set are applied to the same file system location on the device.
Partition	Select a Partition from the drop-down menu. (**Note**: This field is only displayed if you have configured one or more Partitions.) In general, a Partition is a grouping of devices with unique IP addresses. Multiple Partitions can be managed by a single NA Core. A NA Core in an installation of a NA server, comprised of a single Management Engine, associated services, and a single database.
Image 1... 5	You can enter up to five new images or configuration files for the Image Set.
Vendor MD5 Checksum	Enter the vendor’s MD5 checksum. Checksum is a 128-bit checksum computed using the MD5 algorithm. MD5 is a cryptographically secure algorithm. It is very difficult for someone to intentionally change a file and still obtain the same checksum for the file. Frequently, a vendor supplies these checksums along with the software images for their devices. If you compute the checksum on the image (or NA computes it for you), it should match what the vendor supplied. If it does not match, you probably have a corrupted image file which should not be deployed or the vendor may have calculated a checksum using a different algorithm.
ZIP with multiple images	Specify a ZIP compressed file which will be uncompressed. Adding all the files in the ZIP to the Image Set.

Field	Description/Action
Image Set Requirements	Image Set requirements include: • Driver — The driver information to save with the software. The list includes all known drivers. For example, if you want to upload software on a Cisco Aironet 1100 Access Point, select the “Cisco Aironet access points, 350, 1100, and 1200 series, IOS version 12.2” drivers. • Model — The model information to save with the software. The list includes all known models. For example, if you have a Cisco Aironet 1200 series Access Point, select “AIR-AP1220-IOS-UPGRD (C1200 Series).” • System Memory (in bytes) >= — The minimum RAM the image set requires to operate successfully. On most devices, the image resides in processor memory, also known as System Memory or DRAM. The amount of processor memory physically present is calculated for each device using the File System diagnostic. For example, 16,384 bytes equals 16k. Note that not all devices support the File System diagnostic. On those devices, the RAM requirement is ignored. • Processor — The CPU on the device. For example, if you have a Cisco Aironet 1200 series Access Point, select “AIR-AP1220-IOS-UPGRD (PowerPC405GP).” • Boot ROM — The ROM on the device.
Description	Enter a brief description to differentiate this software download from others.

Edit Software Image Page Fields

To edit software images:

1. On the menu bar under Devices, select Device Tools and click Software Images. The Software Images page opens.
2. For the image set you want to edit, click the Edit option in the Actions column. The Edit Software Image Set page opens.

Field	Description/Action
Image Set Name	Displays the name for this image set. You can also specify an existing image set, in which case NA adds the new image to the existing image set. All images in a particular image set are applied to the same file system location on the device.
Partition	Select a Partition from the drop-down menu. (**Note**: This field is only displayed if you have configured one or more Partitions.)
Image Set Requirements	• Driver — The driver information to save with the software. The list includes all known drivers. For example, if you want to upload software on a Cisco Aironet 1100 Access Point, select the “Cisco Aironet access points, 350, 1100, and 1200 series, IOS version 12.2” drivers. • Model — The model information to save with the software. The list includes all known models. For example, if you have a Cisco Aironet 1200 series Access Point, select “AIR-AP1220-IOS-UPGRD (C1200 Series).” • Device RAM Required >= — The minimum RAM of the device. • Processor — The CPU on the device. For example, if you have a Cisco Aironet 1200 series Access Point, select “AIR-AP1220-IOS-UPGRD (PowerPC405GP).” • Boot ROM — The ROM on the device. • Description — A brief description, to differentiate this software download from others.

Be sure to click Save Software when finished.

Deploying Software

The Update Software option enables you to automatically upgrade the current software images installed on your devices. This significantly reduces the time it takes to manually roll out network-wide software upgrades and provides an audit trail for software upgrades to ensure that all policies and procedures are being followed.

To automatically upgrade the current software image on your devices:

1. On the menu bar under Devices, select Device tools and click Software Images. The Software Images page opens.
2. For the image set you want to deploy, click the Update Software option in the Actions column. The Update Device Software task opens. Refer to "Update Device Software Task Page Fields" on page 325 for information.

Keep in mind that:

- Total memory is the total physical memory on the device.
- Free memory is the free memory available for uploads at the time of the last memory diagnostic.
- Net memory is the estimate of free memory after the Update Device Software task is run, taking into account any files you marked to be added or removed from the device (but not taking into account the squeeze pre or post processing task).

Adding a New Software Level

It is very important that your devices are running the latest approved software. Network administrators can group images into categories, such as Pre-production or Obsolete. Images can also classified, for example Security Risk, based on recently discovered vulnerabilities.

To add a new software level or review existing definitions:

1. On the menu bar under Devices, select Device Tools and click Software Images. The Software Images page opens.
2. Click the Software Levels option at the top of the page. The Software Levels page opens.
3. Click the Add Level option. The Add Software Level page opens. Be sure to click Save when finished.

Add Software Level Page Fields

Field	Description/Action
Add Software Level	
Level Name	Enter the level name.
Status	Displays one of the following options: • Active — Marks the configuration policy active (the default). • Inactive — Deactivates the configuration policy. Inactive policies do not generate non-compliance events.
Level	Select a compliance rating name. You can use any of the compliance definitions given depending on your requirements and validation procedures. Options include: • Security Risk • Pre-production • Obsolete • Bronze • Silver • Gold • Platinum
Description	Enter a description of the compliance.
Partition	Select a Partition from the drop-down menu. (**Note**: This field is only displayed if you have configured one or more Partitions.)
Matching Criteria (Matching criteria can use wildcard operators: * and ?.)	
Software Version	Enter the software version currently running on the device.
Device Driver	Select a device driver used to access the device from the drop-down menu. (Any is the default.)

Field	Description/Action
Device Model	Enter the device model.
Filename	Enter a string to match the OS filename.
Configuration Contains	Enter a pattern to match against the current device configuration to determine if the compliance applies to a given device.
Software Vulnerability Information (for Security Risk compliance level)	
Disclosure Date	Enter the date when the software vulnerability was flagged in the following format: *yyyy-MM-dd*.
Importance	Select the severity of the security vulnerability from the drop-down menu, including: • Critical • High • Medium • Low • Informational
CVE Name	Enter the CVE (Common Vulnerabilities and Exposures) name. CVE is a list of standardized names for vulnerabilities and other information on security exposures. (For more information, refer to www.cve.mitre.org.)
Solution	Enter detailed solution information.
Advisory Link	Enter the URL to an external reference for advisory information on a vulnerability.
Solution Link	Enter the URL to an external reference for more information on possible solutions to the vulnerability.

Viewing Device Software Versions

The Device Software report enables you to view the software version and compliance rating currently assigned to each device.

1. On the menu bar under Devices, select Device Tools and click Software Images. The Software Images page opens.
2. Click the Software Levels option at the top of the page. The Software Levels page opens.
3. Click the Device Software Report option at the top of the page. The Device Software Report opens. Refer to "Device Software Report Fields" on page 618 for information.

Note: You can also navigate to the Device Software report from the Reports drop-down menu.

Chapter 10: Event Notification Rules

Use the following table to quickly locate information.

Topic	Refer to:
Getting Started	“Getting Started” on page 456
Adding Event Rules	“Adding Event Rules” on page 461
Event Rule Search Results	“Event Notification & Response Rules Page Fields” on page 461
New Event Notification Rules	“New Event Notification & Response Rules Page Fields” on page 462
Event Rule Variables	“Event Rule Variables” on page 466

Getting Started

HP Network Automation (NA) enables you to trigger many different actions when events occur in the system, including:

- Running tasks, such as snapshots or diagnostics
- Sending Email notification
- Sending Email digests
- Sending SNMP traps
- Sending Syslog messages

Event rules can be limited to specific device groups and/or times of day. The following table describes the available events from which you can select.

Event	Description
Approval Denied	A user has denied an approval request.
Approval Granted	A user has approved a task.
Approval No Longer Required	A task approval is no longer required.
Approval Override	A user has overridden the approval of a task allowing the task to run without approval.
Approval Request	A user has created a task that requires approval before it can run.
Approval Task Changed	A user has made a change to a task that requires approval before it can run.
Approval Task Deleted	A user has deleted a task that was earmarked for approval.
Approval Task Timeout	A task was not approved in the time allotted.
Command Authorization Error	A user tried to run a command that he/she is not authorized to use.
Concurrent Telnet/SSH Session Override	A user ignored the restriction on simultaneous logins. The user logged-in to a device via the Proxy despite another user's prior login.
Policy Added	A user has added a new configuration policy.
Policy Changed	A user has changed a configuration policy.
Policy Non-Compliance	A configuration change violated a policy rule.
Policy Pattern Timeout	A policy pattern took more than 30 seconds to match.
Policy Rule Added	A user has added a new configuration rule.
Policy Rule Changed	A user has changed a configuration rule.
Device Access Failure	NA cannot access a device. This could be due to a bad password or there was no route to the host.
Device Added	A user added a device.
Device Booted	A device was rebooted.

Event	Description
Device Command Script Completed Successfully	A device command script succeeded.
Device Command Script Failed	A device command script failed.
Device Configuration Change	NA detected a configuration change while running a Snapshot task.
Device Configuration Change - No User	NA detected a configuration change by an unknown user.
Device Configuration Deployment	NA successfully deployed a configuration to a device.
Device Configuration Deployment Failure	NA failed to deploy a configuration to a device.
Device Data Failure	NA failed to save a configuration or diagnostic output to the database.
Device Deleted	A user permanently removed a device.
Device Diagnostic Changed	The results of a diagnostic differ from the previous results.
Device Diagnostic Completed Successfully	A device diagnostic succeeded.
Device Diagnostic Failed	A device diagnostic failed.
Device Edited	A user modified a device's information.
Device Flash Storage Running Low	A device’s flash storage is running low.
Device Group Added	A user has added a device group.
Device Group Deleted	A user has deleted a device group.
Device Group Modified	A user modified a device group.
Device Inaccessible	A device is inaccessible.
Device Managed	A user marked a device as Active.
Device Missing From Import	When the Import task is run periodically and given a file of devices to import, this event occurs when a device was included in the file the last time the import occurred, but is no longer included in the file during the current import.
Device Password Change	A user deployed a password change.
Device Password Change Failure	NA failed to deploy a device password change.
Device Permissions - Modified	A device was added to or removed from a group, which changed permissions such that users can modify the device.
Device Permissions - New Device	Someone added a new device to a device group, changing the permissions for users associated with that device group.
Device Reload failed	A device reload failed.
Device Reservation Conflict	There was a device reservation conflict.

Event	Description
Device Snapshot	NA checked a device for a configuration change.
Device Software Change	NA detected a new OS version on a device (for example: from IOS 11 to IOS 12).
Device Startup/Running Config Difference	NA detected a difference between the Startup and Running configurations.
Device Unmanaged	A user marked a device as Inactive. Imported devices can also be Inactive if unreachable for a certain time of period.
Distributed System - Broken Replication Job	NA detected a broken replication job.
Distributed System - Data Synchronization Delay warning	NA detected a data synchronization delay warning.
Distributed System - Deferred LOBs Exceed Threshold	NA detected an excess of deferred LOBs.
Distributed System- Device Software Transfer Error	NA detected a device software transfer error.
Distributed System - Fixed Replication Job	NA detected a fixed replication job.
Distributed System - RMI Error	NA detected a RMI error.
Distributed System - Replication Errors	NA detected replication errors.
Distributed System - Stopped Merge Agent Job	NA detected a stopped merge agent job.
Distributed System - Time synchronization Error	NA detected a time synchronization warning.
Distributed System - undeletable anomalous generations	NA detected undeletable anomalous generations.
Distributed System - uniqueness conflict	NA detected a uniqueness conflict.
Email Report Saved	A user has saved an email report.
External Directory Server Authentication Error	NA could not connect to an external LDAP authentication server.
Last Used Device Password Changed	The password last used for access to a device was changed.
License Almost Exceeded	The devices exceed 90% of the total number of licensed nodes.
License Almost Expired	Your NA license expires soon (date-based licenses only).
License Exceeded	The devices exceed the total number of licensed nodes. NA allows a 20% excess.
License Expired	Your license has expired. NA will no longer allow logins, but will continue to take scheduled snapshots and record changes.

Event	Description
Module Added	Someone added a module/blade/card to a device.
Module Changed	Someone changed the attributes of a module/blade/card installed in a device.
Module Removed	Someone removed a module/blade/card from a device.
Monitor Error	A server monitor failed to run.
Monitor Okay	A server monitor ran successfully.
Pending Task Deleted	A user deleted a scheduled task before it ran.
Reserved Device Configuration Changed	A user has changed the device configuration on a reserved device.
Scheduled for Deploy Configuration Edited	A user modified a configuration that was scheduled to be deployed.
Scheduled for Deploy Password Modified	A new password was deployed, and there is another Password Deploy task scheduled. This indicates that the new password that was just deployed will be changed again (when the pending Password Deploy task executes).
Security alert	NA has detected a security alert.
Server Startup	The NA Management Engine was started.
Session Data Captured	The Proxy saved a connect session to the database.
Software Update Failed	NA failed to update the OS software on a device.
Software Update Succeeded	NA successfully updated the OS software on a device.
Software Vulnerability Detected	If you setup a software level set to “Security Risk,” when NA snapshots devices and detects an OS version that is tagged as a “Security Risk,” this event is generated.
Summary Reports Generated	A user has generated Summary reports.
Task Completed	A task has completed.
Task Started	A task has started.
Ticket Created	When using the HP Remedy AR System Connector (or any of the HP Connectors that interact with a 3rd party Ticketing systems), this event indicates that NA created a ticket in that 3rd party Ticketing system.
User Added	A user has been added.
User Authentication Error	A user entered an incorrect password when logging into NA.
User Authentication Error Lockout	A user is locked out due to too many consecutive failed login attempts.
User Deleted	A user has been deleted

Event	Description
User Disabled	A user record was edited and the user’s status changes from Enabled to Disabled.
User Enabled	A user record was edited and the user’s status changes from Disabled to Enabled.
User Login	A user logged-in to NA.
User Logout	A user has logged-out of NA.
User Message	A user created a message by clicking the New Message link.
User Permission Changed	A user’s permission has been changed.

Adding Event Rules

To add event notification rules, on the menu bar under Admin, click Event Notification & Response Rules. The Event Notification & Response Rules page opens. This page lists currently defined rules that are triggered by NA events. Event rules marked with a pound sign (#) are inactive.

Note: Admin users see all event rules; other users see only their own event rules.

Event Notification & Response Rules Page Fields

Field	Description/Action
New Event Notification & Response Rule link	Opens the New Event Notification & Response Rule page. Refer to "New Event Notification & Response Rules Page Fields" on page 462 for information.
Rule Name	Displays the name of the event rule.
Partition	If you have created Partitions for security or business reasons, you can partition event rules according to Partitions. If the event rule is available to all Partitions, the event rule is labeled "Shared" (or "Global") depending on configuration. Keep in mind that you cannot edit or delete event rules without the proper permissions. Refer to "Segmenting Devices and Users" on page 150 for detailed information on creating Partitions.
Action	Displays the action performed by the event rule. Actions include: • Run Task • Send Email • Send SNMP Trap • Add to Email Digest • Send Syslog Message
Created By	Displays the event rule's owner.
Actions	You can select from the following options: • Edit — Opens the Edit Event Notification & Response Rule page, where you can edit an event rule. Refer to "New Event Notification & Response Rules Page Fields" on page 462 for information. • Delete — Opens a confirmation window, where you are prompted to confirm the deletion. This option appears only when you have permission to delete the event rule.

New Event Notification & Response Rules Page Fields

The New Event Notification & Response Rule page enables you to add/edit a new Event Notification & Response rule.

1. On the menu bar under Admin, click Event Notification & Response Rules. The Event Notification & Response Rules page opens.
2. Click the New Event Notification & Response Rule link at the top of the page. The New Event Notification & Response Rule page opens.

Field	Description/Action
Add Email & Event Rule named	Enter the event rule name.
To take this action	Select one of the following options. (**Note**: Depending on the option you select, the page will refresh and provide specific fields for the action.) • Run Task — Refer to "Run Task Action" on page 463. • Send Email Digest — Refer to "Send Email Digest Action" on page 463. • Send Email Message — Refer to "Send Email Message Action" on page 464. • Send SNMP Trap — Refer to "Send SNMP Trap Action" on page 464. • Send Syslog Message — Refer to "Send Syslog Message Action" on page 465. • Create/Add to Ticket — Refer to "Create/Add to Ticket" on page 465.
When the following events occur	Select one or more of the events from the events list. You can select multiple events using Ctrl+click or Shift+click. Refer to "Getting Started" on page 456 for a description of the event rules. If you select the Configuration Policy Non-Compliance event, select one of the following options: • of any importance — If selected (the default) the event rule will trigger regardless of the importance of any violated configuration policy rules. Refer to "New Rule Page Fields" on page 422 for information on how to set configuration policy rule importance. • of at least < > importance — You can select either Critical, High, Medium (the default), Low, or Informational. The event rule will trigger only if the event was generated due to the failure of a configuration policy rule with an importance equal to or greater than the importance selected. Refer to "New Rule Page Fields" on page 422 for information on how to set configuration rule importance. • For all policies — If selected (the default) all configuration polices are checked. • For selected policies — Select one or more configuration policies from the list. You can use Shift+click or Ctrl+click to select multiple configuration polices. If you select the Device Command Script Completed Successfully or Device Command Script Failed event, you can select a command script from the drop-down menu. If you select the Device Diagnostic Changed or the Device Diagnostic Completed Successfully event, you can select a diagnostic from the drop-down menu.
Rule Status	Select one of the following options: • Active — If checked (the default), the event rule is run when the event occurs. • Inactive — If checked, the event rule is not run. This option can be used to temporarily turn off an event rule.

Field	Description/Action
Between	If checked, specify a time range and select the hours to start and end the event rule.
On devices in this Partition	If partitioning is enabled, select a Partition from the drop-down menu. Refer to “Segmenting Devices and Users” on page 150 for detailed information on creating Partitions.
On devices in these groups	If checked, select one or more groups from the list.

Depending on the action you select, the bottom portion of the New Event Notification & Response Rules page will be different.

Run Task Action

When an event occurs, you can have it trigger any NA task. You can have NA take a snapshot, store diagnostics, run a command script, or even launch an external application. You can even feed event variables into the command line for external applications. This enables you to customize NA and tailor its operations to your needs.

Wait	Enter the number of seconds, minutes, hours, or days to wait before running the task.
Task	Select a task to run from the drop-down menu.

Send Email Digest Action

Email digests combine multiple NA events into a single email report that is sent periodically. Email digests can be used to inform users of common system events, such as configuration changes or device add, delete, and change activity.

You can quickly scan digests for events of interest, while minimizing email volume. Each user can have one email digest. A user can set up multiple event rules. Each rule feeds a different set of events into their digest.

Note: If you want multiple email digests with different schedules or recipient lists, you can create users whose only purpose is to define appropriate digest rules.

Send all my digests starting at (hour)	Enter the hour of the day when you want NA to send your email digests.
And repeating every (hours)	Enter the interval at which you want NA to send your email digests. For example, if you enter 6, the digests are sent every six hours.
From	Enter the email address of the sender. This default is NA.
To	Enter the email address of the recipient. Be sure to separate multiple addresses with commas. Note: If the variable is set to $EventUserEmail$, the email address is derived from the user who created the Email Digest. As a result, if the user’s email address changes, the new email address is used.
Subject	Enter a brief subject line of the message.
Message Header	Enter a message header. This is the text that begins the header or summary section of the message. For HTML messages, this is often an ordered list tag .
End Summary	Enter the text that ends the header or summary section of a message. For HTML messages, this is often an ordered list end tag .

Field	Description/Action
Message Footer	Enter the message footer. You can tailor this to your needs. For example, you could provide contact information or indicate this message is sent by the NA server.
Text Message or HTML Message	Check either Text Message or HTML Message (the default). If you select HTML Message, NA sends the appropriate mail headers so that the mail reader can interpret the HTML in the message. If you select Text Message, NA sends a plain text message, and any HTML tags are displayed as is.
Event Summary	This field provides the summary text, briefly describing the event. The specific message content is unique to the rule. For HTML messages, this line often begins with a list item tag and may contain additional HTML tags and NA variables. If you click the Display Variable Names link, the Event Rule Variables window opens, listing all the variables you can use.
Event Details	This field includes the text, variables, and optional HTML tags that describe the event in detail.
Send Email Message Action	
You can send email messages to users or distribution lists when NA events occur. One email message is sent for each event. For example, you can use this action to alert all users when a core device's configuration changes, to notify a system administrator when a device is inaccessible, or to keep an archive of system events in a public folder. You could also define a text-only event rule with a brief message to email your pager.	
From	Enter the person or process and email address the email message is from. If you click the Display Variable Names link, the Event Rule Variables window opens, which lists all the variables you can use. Refer to “Event Rule Variables” on page 466 for more information.
To	Enter a comma-separated list of email addresses to receive the message. To send email to the user associated with the event, use the variable $EventUserEmail$.
Subject	Enter the subject line of the email message. You can use variables to include system information on the subject line.
Text Message	If checked, NA sends a plain text message. Any HTML tags are displayed as is.
HTML Message	If checked, NA sends the appropriate mail headers so that the mail reader can interpret the HTML in the message.
Both Text and HTML	If checked (the default), both a text message and an HTML message is sent. Keep in mind that NA sends a multi-part email message. The email client displays whichever format is appropriate. For example, Outlook displays HTML by default. If messages are received on a pager, PDA, or similar device, HP recommends using short text-only messages.
Send SNMP Trap Action	
An SNMP Trap is a network status message (defined by RFCs 1155 and 1215). This action is used to send SNMP traps when NA events occur. For example, you can send an SNMP trap to your Network Management System (NMS) every time a snapshot is taken. To display the trap correctly, you may first need to load the NA Management Information Base (MIB), which defines the message format. (**Note**: The network must be configured to permit SNMP traffic to travel through routers, firewalls, and other network devices.)	
SNMP Trap Receiver Hostname	Enter the DNS name or IP address of the host.

Field	Description/Action
SNMP Trap Receiver Port	Enter the host port that receives the SNMP trap. If you click the User Default Port link, the default port number is entered. 162 is the standard SNMP port.
SNMP Community String	Enter the community string to use when sending the SNMP trap. The recipient must be configured to accept this string. If you click the Use Default Community String link, the default community string, Public, is entered.
SNMP Version	Select the version of SNMP to use, either v1 (the default) or v2.
Event Description	Enter a description of the event. You can include NA variables. If you click the Display Variable Names link, the Event Rule Variables window opens, which lists all the variables you can use. Refer to "Event Rule Variables" on page 466 for more information.
Severity	Select one of the following options to identify the severity of the event. Note that there is no intrinsic security level associated with each event, so you can assign any value that makes sense. • Alert • Critical • Debug • Emergency • Error • Info • Notice • Warning
Send Syslog Message Action	
You can use syslog messages to forward any NA event to an external management system. For example, you might notify your CA UniCenter system when NA detects a device configuration change so that an alert appears on your operations console.	
Syslog Hostname	Enter the host name of the Syslog server.
Syslog Port	Enter the port used by Syslog. If you click the Use Default Port link, the default Syslog port, 514, is entered.
Syslog Message	Enter the Syslog message, including variables. If you click the Display Variable Names link, the Event Rule Variables window opens, which lists all the variables you can use. Refer to "Event Rule Variables" on page 466 for more information.
Create/Add to Ticket	
Ticketing System Hostname	Enter the ticketing system hostname.
Event Description	Enter the event description.

Be sure to click Save Rule when you are finished.

Event Rule Variables

Several event rule variables are available for:

- Device events
- Device configuration events
- Device diagnostics events
- Task events
- All events

Device Events Variables

Note: Variables are case-sensitive. You must enter them exactly as shown.

You can use these variables only for device event rules:

Variable	Description
$DeviceID$	NA's identification number for the device.
$HostName$	The device's host name.
$IPAddress$	The devices primary IP address.
$FQDN$	The devices fully-qualified domain name.
$Vendor$	The device's manufacturer.
$Model$	The device's model number.

Variables for Device Configuration Events

Note: Variables are case-sensitive. You must enter them exactly as shown.

You can use these variables only for device configuration event rules:

Variable	Description
$DataID$	NA's identification number for the latest configuration
$Comments$	Configuration comments.
$Diff$	Textual differences of the configuration changes.

Variables for Device Diagnostic Events

Note: Variables are case-sensitive. You must enter them exactly as shown.

You can use these variables only for device diagnostics event rules:

Variable	Description
$CurrentDiag$	The text of the current diagnostic.
$PreviousDiag$	The text of the previous diagnostic.
$Diff$	The textual difference of the changes between current and previous diagnostic.
$DataID$	Indicates that it is also for diagnostic events.

Task Event Variables

Note: Variables are case-sensitive. You must enter them exactly as shown.

You can use these variables only for device diagnostics event rules:

Variable	Description
$ApprovalDate$	Task approval date.
$ApproverEmails$	Comma separated list of email addresses of the task approvers.
$ApprovalPriority$	Task approval priority.
$OriginatorFirstName$	The first name of the task originator.
$OriginatorLastName$	The last name of the task originator.
$OriginatorName$	The name of the task originator.
$TaskName$	The task name.
$TaskComments$	The task comments.
$TaskDevices$	A list of devices affected by the task.
$TaskFrequency$	The frequency of the task.
$TaskID$	The task identifier.

Variables for All Events

You can use the following variables in all event rules. Keep in mind Variables are case-sensitive. You must enter them exactly as shown. (**Note**: For a complete list of variables, click the Display Variable Names link on the New Event Notification & Response Rule page.)

Variable	Description
$AppURL$	NA's application URL (such as *https://host/*) used to put links to NA directly into email messages.
$EventID$	The NA identification number of this event.
$EventType$	The type of event.
$EventDate$	The date the event occurred.
$EventText$	The event details.
$EventUserFirstName$	The first name of the NA user associated with this event. (Note: If no user is associated with this event or if no First Name is set for the user, this will be an empty string.)
$EventUserLastName$	The last name of the NA user associated with this event. (Note: If no user is associated with this event or if no Last Name is set for the user, this will be an empty string.)
$EventUserName$	The NA user name associated with this event (indicates "no user" when appropriate).
$EventUserEmail$	Email address of the user associated with this event.
$FyiEmails$	Comma separated list of email addresses of the task FYI recipients.
$LocalHostName$	The hostname of the NA server.
$LocalHostAddress$	The IP address of the NA server.

Chapter 11: Performing Searches

Use the following table to quickly locate information.

Search	**Refer to:**
Searching configuration text	“Using the Full-Text Search Functionality” on page 472
Searching for Devices	“Searching for Devices” on page 474
Searching for Interfaces	“Searching for Interfaces” on page 482
Searching for Modules	“Searching for Modules” on page 485
Searching for Policies	“Searching for Policies” on page 488
Searching for Compliance	“Searching for Policy, Rule, and Compliance” on page 491
Searching for Configurations	“Search For Configuration Page Fields” on page 496
Searching for Diagnostics	“Searching for Diagnostics” on page 500
Searching for Tasks	“Searching for Tasks” on page 504
Searching for Sessions	“Searching for Sessions” on page 513
Searching for Events	“Searching for Events” on page 517
Event Descriptions	“Event Descriptions” on page 520
Searching for Users	“Searching for Users” on page 525
Searching for ACLs	“Searching for ACLs” on page 527
Searching for MAC Addresses	“Searching for MAC Addresses” on page 531
Searching for IP Addresses	“Searching for IP Addresses” on page 535
Searching for VLANs	“Searching for VLANs” on page 538
Searching for Device Templates	“Searching for Device Templates” on page 541
SingleSearch	“SingleSearch” on page 544
Advanced Search	“Advanced Search” on page 547

Using the Full-Text Search Functionality

After full-text search is enabled, faster configuration text search is available for the following report options:

- Reports > Search For > Devices > Configuration Text > contains (full text)
- Reports > Search For > Configurations > Configuration Text > contains (full text)
- Reports > Search For > Device Templates > Configuration Text > contains (full text)
- Reports > Advanced Search > Search Criteria > Configuration Text > contains (full text)

Additionally, you can create a dynamic group based on the results of a Search Criteria > Configuration Text > contains (full text) search.

Similarly, these searches also support searching for configuration text that **does not contain (full text)**. The search is always case-insensitive for the **contains (full text)** and **does not contain (full text)** operators. For information about the search types that these operators support, see the "contains (full text) and does not contain (full text) Usage" table.

contains (full text) and does not contain (full text) Usage

Search Type	Notes	Examples
Search for a single word	A word is a sequence of characters containing no spaces.	• interface • telnet • snmp
Search for a single word using the wildcard	The asterisk character (*) is the only supported wildcard; this wildcard must be at the end of the search phrase.	• interf* • tel*
Search for an IP address	IP address searches are treated the same as a single word searches. The asterisk character (*) is the only supported wildcard; this wildcard must be at the end of the search phrase.	• 10.11.12.13 results in an exact match • 10.11.12.* results in all addresses that start with 10.11.12 • 10.11.* results in all addresses that start with 10.11 • fe80:0000:0000:0000:0202:b3ff:fe1e:8329 results in an exact match • fe80:0000:0000:0000:0202:b3ff:fe1e:* results in all address that that start with fe80:0000:0000:0000:0202:b3ff:fe1e • fe80:0000:0000:0000:0202:b3ff:* results in all addresses that start with fe80:0000:0000:0000:0202:b3ff
Search for a phrase	A phrase is a sequence of characters containing one or more white spaces.	• set vlan • set vpn name

contains (full text) and does not contain (full text) Usage (cont'd)

Search Type	Notes	Examples
Search for a phrase using the wildcard	• The asterisk character (*) is the only supported wildcard; this wildcard must represent one or more complete words within of the search phrase. • The * must *not* be at the end of the search phrase. • Use white space on either side of the *. If white space is absent, NA treats the search as a word using the wildcard.	• set * name • telnet * table * settings **Note**: Logical operators (AND, OR, NOT, ACCUM, EQUIV) are not supported nor considered as part of search strings.

Searching for Devices

Device searches enable you to search for devices using a combination of criteria and operators. You can also search for devices that are out of compliance with specified policies or rules. (Refer to "Creating a Policy" on page 416 for information on Policies.)

To search for devices, on the menu bar under Reports select Search For and click Devices. The Search For Device page opens. When you are finished entering search criteria, click the Search button. NA returns a list of devices containing all the specified search criteria on the Device Search Results page. Refer to "Device Search Results Page Fields" on page 480 for information.

Note: When entering search criteria, your settings are lost if you change to a different page before running the search.

Search For Device Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to select the information you want to include in the Device Search Results page.
Host Name	Select an operator and enter the Host Name. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Device IP	Select an operator and enter the device's IP address.
Secondary IP Address	Select an operator and enter the device's secondary IP address.
Device Vendor	Select an operator and enter the name of the vendor who manufactured the device.
Device Model	Select an operator and enter the model designation of the device.
Device Type	Select the type of network device, such as router, switch, firewall, VPN, Virtual Switch, DialUp, DSL_ISDN, WAN, Wireless AP, or load balancer from the scroll-down menu.
Device Status	Select from the following options for the device: • Active • Inactive • Pre-Production (A pre-production device is a device that is not yet active in the production network. Refer to "Bare Metal Provisioning" on page 118 for information.)
Driver Name	Select one or more drivers associated with the device from the scroll-down menu. To select multiple drivers, click the first driver, then Ctrl+click to select additional drivers.
FQDN	Select an operator and enter a Fully Qualified Domain Name (FQDN).

Field	Description/Action
Policy Compliance	Select from the following options for the device: • Any (the default) • Device in compliance • Device not in compliance • Device has no applicable policy • Non-Compliant based on Rule Priority — Select a rule priority from the drop-down menu. You can select Critical, High, Medium, Low, or Informational. This enables you to filter the search to include only devices that are in violation of configuration rules above a given importance. (Refer to "New Rule Page Fields" on page 422 for information on importance ratings for configuration policy rules.) • Non-Compliant with Selected Policies — Select one or more policies from the list. • Non-Compliant with Selected Rules — Select one or more rules from the list. (Refer to "New Rule Page Fields" on page 422 for information on policy rules.)
Access Methods	Select an access method from the scroll-down menu: • FTP • RLogin • SCP • SNMP • SSH • TFTP • Telnet
Device Location	Select an operator and enter the location of the device.
Serial Number	Select an operator and enter the serial number of the device.
Asset Tag	Select an operator and enter information from the device asset tag.
Device Software Version	Select an operator and enter the version number of the operating system running on the device.
Device Firmware Version	Select an operator and enter the version number of the firmware running on the device.
Device Description	Select an operator and enter a description.
Comments	Select an operator and enter a unique portion of the comment for the device. This field is case-sensitive unless the tips at the top of the page indicate that *all* text field searches are case-insensitive.
Free Ports	Select an operator (equals, is less than, or is greater than) and enter the number of free ports.
Percentage of Free Ports	Select an operator (equals, is less than, or is greater than) and enter a percentage of free ports.

Field	Description/Action
Total Ports	Select an operator (equals, is less than, or is greater than) and enter the total number of ports on the device.
Ports In Use	Select an operator (equals, is less than, or is greater than) and enter the number of ports in use.
Percentage of Ports In Use	Select an operator (equals, is less than, or is greater than) and enter a percentage of ports in use.
System Memory	Select an operator (equals, is less than, or is greater than) and enter the total amount of RAM (MB) on the device.
Uptime	Select an operator (is less than or is greater than) and enter the total amount of days. The total number of days, hours, minutes, and seconds since the device was last rebooted is shown on the Device Search Results page. **Note**: Uptime data is collected during the NA Detect Device Boot diagnostic. For the uptime data to be reliable, a recurring diagnostic task must be in place that routinely collects this data. Not all devices support the NA Detect Device Boot Diagnostic. Devices that do not support the diagnostic, as well as devices that have never had the diagnostic run, will have empty fields for Uptime and Uptime Store Date. For information on the Run Diagnostics task, refer to "Run Diagnostics Task Page Fields" on page 312.
Uptime Stored Date	Select an operator (since or until) and then select a timeframe from the pull-down menu. Anytime is the default. You can use the calendar option to select a specific day. The last time NA Detect Device Boot diagnostic was run is shown in the Device Search Results page. For information on the NA Detect Device Boot diagnostic, refer to "View Menu Options" on page 203. **Note**: Uptime data is collected during the NA Detect Device Boot diagnostic. For the uptime data to be reliable, a recurring diagnostic task must be in place that routinely collects this data. Not all devices support the NA Detect Device Boot Diagnostic. Devices that do not support the diagnostic, as well as devices that have never had the diagnostic run, will have empty fields for Uptime and Uptime Stored Date.

Field	Description/Action
Configuration Text	Select an operator, and then enter a unique portion of the device configuration on which to search. • The "contains" and "does not contain" operators support regular expressions, including the ? and * wildcards. These searches are case-sensitive unless the tips at the top of the page indicate that *all* text field searches are case-insensitive. • The "contains (full text)" and "does not contain (full text)" operators support the * wildcard only. For more information, see "Using the Full-Text Search Functionality" on page 472. These searches are always case-insensitive. (**Note**: These operators require that full-text search is enabled for the database.) • IPv6 address shorthand notation (double colon) cannot be used in combination with wildcards. If the search operator is "contains" or "contains (full text)," you can provide a value in the "Show <#> context lines around the matched line when displaying Current Configuration" check box at the bottom of the page. You can include up to five lines above and below the search text in the results page. The default value is three. (**Note**: When the number of results to load is large, showing context lines can significantly slow performance.)
Different Startup/Running	If checked, search devices with different startup and running configuration.
Last Changed Time	Select the following operators: • Since or Until • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.
Create Date	Select the following operators: • Since or Until • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.
Password Rule	Select an operator and enter a Password Rule Name.
ACL ID	Select an operator and enter an ACL ID.
ACL Handle	Select an operator and enter an ACL handle.
ACL Type	Select an operator and enter an ACL type.
ACL Configuration	Select an operator and enter an ACL type. This field is case-sensitive unless the tips at the top of the page indicate that *all* text field searches are case-insensitive.
ACL Application	Select an operator and enter an ACL application. This field is case-sensitive unless the tips at the top of the page indicate that *all* text field searches are case-insensitive.

Field	Description/Action
Module Slot	Select an operator and enter a module slot.
Module Description	Select an operator and enter a module description.
Module Model	Select an operator and enter a module model.
Module Serial	Select an operator and enter a module serial.
Module Memory	Select an operator and enter module memory.
Module Firmware Version	Select an operator and enter the module's firmware version.
Module Hardware Revision	Select an operator and enter the module's hardware revision.
ROM Version	Select an operator and enter the module's ROM version. The ROM version is the version of the bootstrap code used in ROM to instruct the device on how to boot and load the operating system.
Service Type	Select an operator and enter a service type.
Custom Service Type	Select an operator and enter a custom service type.
VTP Domain Name	Select an operator and enter a VLAN Trunking Protocol (VTP) domain name.
VTP Operating Mode	Select an operator and enter a VLAN Trunking Protocol (VTP) operating mode.
Device Custom Data	Select an operator and enter the unique text that might appear in any of the custom fields that are listed. (**Note**: This section is not displayed if there are no custom fields.)
Device belongs to	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use the Device Selector to select groups. For information on how to use the Device Selector, refer to "Device Selector" on page 144.
Partition	Select a Partition to limit search results to devices in that Partition. The Default Partition (named Default Site) initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Partitions. Refer to "Partitions" on page 158 for detailed information on Partitions.)

When you click the Search button, NA returns a list of devices containing all the specified search criteria on the Device Search Results page. Refer to "Device Search Results Page Fields" on page 480 for information.

Device Search Results Page Fields

The Device Search Results page display depends on the search criteria that you selected on the Search For Devices page. Refer to "Search For Device Page Fields" on page 475 for information on search criteria. The following table describes the available options on the Device Search Results page.

Option	Description/Action
Modify this search link	Returns you to the Search For Device page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Check Boxes	You can use the left-side check boxes to manage devices. Once you have selected the devices, click the Actions drop-down menu and click either: • Activate — Instructs NA to manage the selected devices. • Deactivate — Instructs NA not to manage the selected devices. • Batch Edit — Opens the Batch Edit page. Refer to "Batch Edit Device Page Fields" on page 163. • Diagram — Refer to "Diagramming" on page 609. • Delete — Deletes the selected devices. • Check Policy Compliance — Refer to "Check Policy Compliance Task Page Fields" on page 374. • Configure Syslog — "Configure Syslog Task Page Fields" on page 286. • Deploy Passwords — "Deploy Passwords Task Page Fields" on page 290. • Discover Driver — "Discover Driver Task Page Fields" on page 295. • Reboot Device — "Reboot Device Task Page Fields" on page 298. • Run Command Script — "Run Command Script Task Page Fields" on page 306. • Run Diagnostics — "Run Diagnostics Task Page Fields" on page 312. • Run ICMP Test — "Run ICMP Test Task Page Fields" on page 301. • Take Snapshot — "Take Snapshot Task Page Fields" on page 317. • Synchronize Startup and Running — "Synchronize Startup and Running Task Page Fields" on page 321. • Update Device Software — "Update Device Software Task Page Fields" on page 325. • Delete ALCs — "Delete ACLs Task Page" on page 698. • OS Analysis — "OS Analysis Task Page Fields" on page 352. • Provision Device — Refer to "Edit Device Page Fields" on page 113. The adjacent Select drop-down menu enables you to select or deselect all of the devices.

Option	Description/Action
Actions	You can select the following actions for each entry in the Device Search Results table: • Edit — Opens the Edit Device page, where you can edit information about this device. • Telnet — Opens a Telnet window to the NA CLI. NA will attempt to log you into the device. • SSH — Opens an SSH window to NA CLI. NA will attempt to log you into the device. • View Config — Opens the Current Configuration page, where you can edit and add comments to the selected configuration. •
Search Criteria	Displays the search criteria used in the search. You can: • Save as a new device group — Select either "All Result Devices" or "Selected Devices Only," enter the name of the new device group, and click Create Group. • Add to an existing static device group — Select either "All Result Devices" or "Selected Devices Only," select a device group from the drop-down menu, and click Add. • Save search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. Refer to "User & System Reports" on page 599 for information. • Email Search Result - Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as CSV File - Downloads the search results in CSV format.

Searching for Interfaces

You use interface searches to search the NA database for information on interfaces installed in your devices. Keep in mind that although a Port is a Layer 2 term and Interface is a Layer 3 term, NA does not make that distinction.

To search for interfaces, on the menu bar under Reports select Search For and click Interfaces. The Search For Interface page opens. When you are finished entering search criteria, click the Search button. NA returns a list of interfaces containing all the specified search criteria on the Interface Search Results page. Refer to “Interface Search Results Page Fields” on page 484 for information.

Note: When entering search criteria, your settings are lost if you change to a different page before running the search.

Search For Interface Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to select the information you want to include in the Interface Search Results page.
Port Name	Select an operator and enter the port’s name, such as Ethernet0 or Serial1. A port is defined as a single endpoint defined as a combination of a binding and a network address. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal
Port IP	Select an operator and enter the port IP.
CIDR Range	Select an operator and enter the port’s Classless Inter-Domain Routing (CIDR) range, for example: 192.168.1.0-192.168.2.0 or 192.168.31.0/24). Keep in mind that CIDR ranges are inclusive.
Port Type	Select an operator and enter the port type, such as Ethernet, FastEthernet, or PortChannel.
Port Status	Select an operator and enter the port’s status, such as Configured Up or Administratively Down.
Running Port State	Displays if the port is Configured Up or Administratively Down. (**Note**: This does not reflect the protocol state of the port, only the configured state.)
Description	Select an operator and enter the port’s description.
Configured Duplex	Select and operator and enter the port’s configured duplex setting.
Configured Speed	Select and operator and enter the port’s configured speed setting.
Negotiated Duplex	Select an operator and enter the port’s detected duplex setting.

Field	Description/Action
Negotiated Speed	Select an operator and enter the port's detected speed setting.
VLAN Name	Select an operator and enter the port's VLAN name. The VLAN name is the name of the VLAN, for example VLAN2 or VLAN3, on which to limit the search.
Host Name	Select an operator and enter the device's Host Name. Keep in mind that you can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Device IP	Select an operator and enter the device's IP address.
Module Slot	Select an operator and enter a module slot number.
Module Description	Select an operator and enter the module's description.
Module Model	Select an operator and enter the module's model number.
Module Serial	Select an operator and enter the module's serial number.
Module Firmware Version	Select an operator and enter the module's firmware version.
Interface Custom Data	Select an operator and enter the unique text that might appear in any of the custom fields that are listed. (**Note**: This section is not displayed if there are no custom fields.)
Device belongs to	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use the Device Selector to select groups. For information on how to use the Device Selector, refer to "Device Selector" on page 144.
Partition	Select a Partition to limit search results to devices in that Partition. The Default Partition (named Default Site) initially includes all of Inventory. (**Note**: This field is only displayed if you have configured multiple Partitions. Refer to "Partitions" on page 158 for detailed information on Partitions.)

Interface Search Results Page Fields

The Interface Search Results page display depends on the search criteria that you selected on the Search For Interface page. Refer to "Search For Interface Page Fields" on page 482 for information on search criteria. The following table describes the available options on the Interface Search Results page.

Option	Description/Action
Modify this search link	Returns you to the Search For Interface page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Check Boxes	You can use the left-side check boxes to select interfaces. Once you have selected an interface, click the Actions drop-down menu and click Run Interface Script. The New Task - Run Command Script page opens. Refer to "Running Command Scripts" on page 596 for information. The adjacent Select drop-down menu enables you to select or deselect all of the interfaces.
Actions	You can select the following actions for each entry in the Interface Search Results table: • Edit Interface — Opens the Edit Interface Detail page, where you can edit information about this interface. Refer to "Edit Interface Detail Page Fields" on page 210 for information. • View Interface — Opens the Interface Detail page, where you can view interface details. Refer to "Interface Detail Page Fields" on page 208 for information.
Search Criteria	Displays the search criteria used in the search. You can: • Save search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. Refer to "User & System Reports" on page 599 for information. • Email Search Result - Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as CSV File - Downloads the search results in CSV format.

Searching for Modules

You use module searches to search the NA database for information on the cards, blades, or modules installed in your devices.

To search for modules, on the menu bar under Reports, select Search For and click Modules. The Search For Module page opens. When you are finished entering search criteria and click the Search button, NA returns a list of modules containing all the specified search criteria on the Module Search Results page. Refer to "Searching for Policies" on page 488 for information.

Note: When entering search criteria, your settings are lost if you change to a different page before running the search.

Search For Module Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the Module Search Results page to show only the selected information.
Host Name	Select an operator and enter the Host Name. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Device IP	Select an operator and enter the device's IP address.
Module Slot	Select an operator and enter the slot on the device in which the module is installed.
Module Description	Select an operator and enter a unique portion of the module's description.

Field	Description/Action
Module Model	Select an operator and then enter the model of the module. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the “equals” and “does not equal” operators.)
Module Serial	Select an operator and enter the module’s serial number.
Module Memory	Select an operator and enter the total amount of RAM (MB) on the module.
Module Firmware Version	Select an operator and enter the version number of the firmware loaded on the module.
Module Hardware Revision	Select an operator and enter a portion of the module’s hardware revision designation.
Comments	Select an operator and enter a portion of the module’s comment. This field is case-sensitive unless the tips at the top of the page indicate that *all* text field searches are case-insensitive.
Module Custom Data	Select an operator and enter the unique text that might appear in any of the custom fields that are listed. (**Note**: This section is not displayed if there are no custom fields.)
Device belongs to	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use the Device Selector to select groups. For information on how to use the Device Selector, refer to “Device Selector” on page 144.
Partition	Select a Partition to limit search results to devices in that Partition. The Default Partition (named Default Site) initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Partitions. Refer to “Partitions” on page 158 for detailed information on Partitions.)

Module Search Results Page Fields

The Module Search Results page display depends on the search criteria that you selected on the Search For Module page. Refer to "Search For Module Page Fields" on page 485 for information. The following table describes the available options on the Module Search Results page.

Option	Description/Action
Modify this search link	Returns you to the Search for Module page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Actions	You can select the following actions for each entry in the Module Search Results table: • Edit Module — Opens the Edit Blade/Module Detail page, where you can edit information about this module. • View Module — Opens the Blade/Module Detail page, where you can view module details.
Search Criteria	Displays the search criteria used in the search. You can: • Save as a new device group — Select either "All Result Devices" or "Selected Devices Only," enter the name of the new device group, and click Create Group. • Add to an existing static device group — Select either "All Result Devices" or "Selected Devices Only," select a device group from the drop-down menu, and click Add. • Save search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. Refer to "User & System Reports" on page 599 for information. • Email Search Result - Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as CSV File - Downloads the search results in CSV format.

Searching for Policies

The NA Policy Manager applies a set of rules, or filters, to each device configuration change that NA detects. If a change to a device (or group of devices) is non-compliant, the NA Policy Manager generates an event which can trigger a notification rule. As a result, you can correct the non-compliant change, preserving both compliance and network availability. Refer to "Creating a Policy" on page 416 for detailed information on Policy Management. For information on the auto-remediation feature, refer to "How the NA Policy Manager Works" on page 415.

The Search for Policies page enables you to narrow down that list of policies you want to view. This enables you to:

- Easily generate a list of policies in NA by using policy attributes as search criteria.
- Easily manage the policies in NA.

If you want to view all of your current polices, on the main menu bar under Policies, click Policy List. Refer to "Policies Page Fields" on page 417 for information.

To search for policies, on the menu bar under Reports, select Search For and click Polices. The Search For Polices page opens. When you are finished entering search criteria, click the Search button. NA returns a list of policies containing all the specified search criteria on the Policies Search Results page.

Note: When entering search criteria, your settings are lost if you change to a different page before running the search.

Search For Polices Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the Policies Search Results page to show only the selected information.
Policy Name	Select an operator and enter the policy name. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal
Device Group	Select a device group the match the policy scope to be searched Use the Device Selector to select groups. For information on how to use the Device Selector, refer to "Device Selector" on page 144.
Create Date	Select the following operators: • Since or Until • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.

Field	Description/Action
Status	Select one of the following operators: • Any (default) • Active • Inactive
CVE	Enter the CVE (Common Vulnerabilities and Exposures) name, along with an operator. CVE is a list of standardized names for vulnerabilities and other information on security exposures.
Disclosure Date	Select the following operators: • Since or Until • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.
Solution	Enter the solution text, along with an operator. This field is case-sensitive unless the tips at the top of the page indicate that *all* text field searches are case-insensitive.
Vendor URL	Enter a URL to an external reference for more information on the vulnerability, along with an operator.
Solution URL	Enter a URL to an external reference for more information on possible solutions to the vulnerability, along with an operator.
Policy Tag	Select the policy tag on which to search. Policy tags enable you to search for compliance entries related to policies with selected tags.
Partition	Select a Partition to limit search results to devices in that Partition. The Default Partition (named Default Site) initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Partitions. Refer to "Partitions" on page 158 for detailed information on Partitions.)

Policies Search Results Page Fields

The Policies Search Results page displays the search criteria you selected on the Search For Policies page. Refer to “Search For Polices Page Fields” on page 488 for information.

Option	Description/Action
Check Boxes/Drop-down Menus	You can use the left-side check boxes to manage devices. Once you have selected the devices, click the Actions drop-down menu and click either: • Activate — Instructs NA to manage the selected devices. • Deactivate — Instructs NA not to manage the selected devices. • Batch Edit — Opens the Batch Edit Policies page, where you can modify the selected policies’ scope, add device exceptions, and set their (policies’) status. • Delete — Deletes the selected devices.
Modify this search link	Returns you to the Search For Policies page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Actions	You can select the following action for each policy: • View & Edit — Opens the Edit Policy page, where you can modify policies. • Test — Opens the Test Policy page. Refer to “Test Policy Compliance Page Fields” on page 441 for information.
Search Criteria	Displays the search criteria used in the search. You can: • Save search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. Refer to “User & System Reports” on page 599 for information. • Email Search Result - Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as CSV File - Downloads the search results in CSV format.

Searching for Policy, Rule, and Compliance

The Search for Policy, Rule, and Compliance page enables you to search for devices and their associated compliance and applicable policies and rules. This enables you to:

- Easily generate a list of devices that are in or out of compliance.
- Easily generate a list of devices that have not been checked yet by a specific policy rule.
- Identify devices for which a policy rule applies.
- Identify which policy rules apply to specific devices.
- Identify which devices do not have any applicable policies.

Note: On this page, you cannot search for policies or rules independent of devices.

To search for policies, policy rules, and compliance violations, on the menu bar under Reports, select Search For and click Compliance. The Search For Policy, Rule, and Compliance page opens. When you are finished entering search criteria, click the Search button. NA returns a list of devices containing all the specified search criteria on the Policy, Rule, and Compliance Search Results page.

Note: When entering search criteria, your settings are lost if you change to a different page before running the search.

Search For Policy, Rule, and Compliance Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the Policies Search Results page to show only the selected information.
Host Name	Select an operator and enter the Host Name. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the “equals” and “does not equal” operators.)
Device IP	Select an operator and enter the device’s IP address.
Device Group	Use the Device Selector to select groups. For information on how to use the Device Selector, refer to “Device Selector” on page 144.
Compliance	Select one of the following options: • Any compliance state • Device in compliance • Device not in compliance • Device not checked yet • Device has no applicable policy
Policy	Enter the name of the policy or select a policy from the drop-down menu.
Rule	Enter a policy configuration rule or select one from the drop-down menu.
Rule Type	Select one or more of the following options: • Configuration • Diagnostics • Software
Rule Importance	Select one or more Importance levels. Options include: • Informational — Events that typically do not require a response. • Low — Events that may require a response as time permits. • Medium — Events that require a timely response, typically within 72 hours. • High — Events that require an urgent response, typically within 24 hours. • Critical — Events that require an immediate response.
Rule Description	Include rule description in search results.

Field	Description/Action
CVE	Enter the CVE (Common Vulnerabilities and Exposures) name, along with an operator. CVE is a list of standardized names for vulnerabilities and other information on security exposures.
Last Checked Date	Select the following operators: • Since or Until • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.
Rule Out Of Compliance Date	The rule out of compliance date is the time that NA detects that a device is out of compliance with a particular rule. Select the following operators: • Since or Until • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.
Policy Tag	Select a Policy Tag. Policy tags enable you to search for compliance entries related to policies with selected tags.
Partition	Select a Partition to limit search results to devices in that Partition. The Default Partition (named Default Site) initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Partitions. Refer to "Partitions" on page 158 for detailed information on Partitions.)

Policy, Rule, and Compliance Search Results Page Fields

The Policy, Rule, and Compliance Search Results page displays the search criteria you selected on the Search For Policy, Rule, and Compliance page. Refer to “Search For Policy, Rule, and Compliance Page Fields” on page 492 for information.

Option	Description/Action
Check Boxes/Drop-down Menus	You can use the left-side check boxes to manage devices. Once you have selected a device(s), click the Actions drop-down menu and select an action, for example: • Activate — Instructs NA to manage the selected devices. • Deactivate — Instructs NA not to manage the selected devices. • Batch Edit — Opens the Batch Edit Device page, where you can assign a driver and set the connection methods for all of the selected devices. • Diagram — Refer to “Diagramming” on page 609. • Delete — Deletes the selected devices. • Check Policy Compliance — Refer to “Check Policy Compliance Task Page Fields” on page 374. • Configure Syslog — Refer to “Configure Syslog Task Page Fields” on page 286. • Deploy Passwords — Refer to “Deploy Passwords Task Page Fields” on page 290. • Discover Driver — Refer to “Discover Driver Task Page Fields” on page 295. • Reboot Device — “Reboot Device Task Page Fields” on page 298. • Run Command Script — “Run Command Script Task Page Fields” on page 306. • Run Diagnostics — “Run Diagnostics Task Page Fields” on page 312. • Run ICMP Test — “Run ICMP Test Task Page Fields” on page 301. • Take Snapshot — “Take Snapshot Task Page Fields” on page 317.
Check Boxes/Drop-down Menus (*continued*)	• Synchronize Startup and Running — “Synchronize Startup and Running Task Page Fields” on page 321. • Update Device Software — “Update Device Software Task Page Fields” on page 325. • Delete ALCs — “Delete ACLs Task Page” on page 698. • OS Analysis — “OS Analysis Task Page Fields” on page 352. • Provision Device — Refer to “Edit Device Page Fields” on page 113.
View Detailed CVS Report	Enables you to create a CSV file with all of the records, including the event detail that explains why the compliance failed.
Modify this search link	Returns you to the Search For Policy, Rule, and Compliance page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.

Option	Description/Action
Search Criteria	Displays the search criteria used in the search. You can: • Save as a new device group — Select either “All Result Devices” or “Selected Devices Only,” enter the name of the new device group, and click Create Group. • Add to an existing static device group — Select either “All Result Devices” or “Selected Devices Only,” select a device group from the drop-down menu, and click Add. • Save search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. Refer to “User & System Reports” on page 599 for information. • Email Search Result - Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as CSV File - Downloads the search results in CSV format.

Searching for Configurations

Configuration searches enable you to search configuration files using a combination of criteria and operators. All search criteria are joined by the Boolean operators AND/OR and the results match all criteria.

To search for configuration files, on the menu bar under Reports, select Search For and click Configurations. Keep in mind that when entering search criteria, your settings are lost if you change to a different page before running the search.

Note: When searching with a criterion that includes configurations, if you have a lot of stored configurations, the query could be slow. It is recommended that you select the "include" option when searching configurations. As a result, the full text search features of either the Oracle or SQL Server database are used.

When you are finished entering your search criteria and click the Search button, NA returns a list of configurations containing all the specified search criteria on the Configuration Search Results page. Refer to "Configuration Search Results Page Fields" on page 499 for information.

Search For Configuration Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the Configuration Search Results page to show only the selected information.
Host Name	Select an operator and then enter the host name of the device. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Device IP	Select an operator and then enter the IP address of the device.
Date	Select the following operators: • Since or Until • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.
Changed By	Select an operator and then enter the login name of a user who might have changed a device's configuration.

Field	Description/Action
Device Status	Select from the following options for the device: • Active • Inactive • Pre-Production (A pre-production device is a device that is not yet active in the production network. Refer to "Bare Metal Provisioning" on page 118 for information.)
Device Type	Select the type of network device, such as router, switch, firewall, VPN, DialUp, DSL_ISDN, or load balancer from the scroll-down menu.
Comments	Select an operator (contains or does not contain) and then enter the comment text you want to find. This searches only text that appears in the Configuration Comment box in the Device Configuration Detail page. This field is case-sensitive unless the tips at the top of the page indicate that *all* text field searches are case-insensitive.
Configuration Text	Select an operator, and then enter a unique portion of the device configuration on which to search. • The "contains" and "does not contain" operators support regular expressions, including the ? and * wildcards. These searches are case-sensitive unless the tips at the top of the page indicate that *all* text field searches are case-insensitive. • The "contains (full text)" and "does not contain (full text)" operators support the * wildcard only. For more information, see "Using the Full-Text Search Functionality" on page 472. These searches are always case-insensitive. (**Note**: These operators require that full-text search is enabled for the database.) • IPv6 address shorthand notation (double colon) cannot be used in combination with wildcards. If the search operator is "contains" or "contains (full text)," you can provide a value in the "Show <#> context lines around the matched line when displaying Current Configuration" check box at the bottom of the page. You can include up to five lines above and below the search text in the results page. The default value is three. (**Note**: When the number of results to load is large, showing context lines can significantly slow performance.)
Search Scope	Check one of the following options: • Search current configurations Only — If checked, only the current configuration is searched. • Search all configurations — If checked, all of the current and historical configurations are searched.
Different Startup/Running	If checked, search devices with different startup and running configuration.
Configuration Custom Data	Select an operator and enter the unique text that might appear in any of the custom fields that are listed. (**Note**: This section is not displayed if there are no custom fields.)

Field	Description/Action
Device belongs to	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use the Device Selector to select groups. For information on how to use the Device Selector, refer to "Device Selector" on page 144.
Partition	Select a Partition to limit search results to devices in that Partition. The Default Partition (named Default Site) initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Partitions. Refer to "Partitions" on page 158 for detailed information on Partitions.)

Configuration Search Results Page Fields

The Configuration Search Results page display depends on the search criteria you selected on the Search For Configuration page. Refer to "Search For Configuration Page Fields" on page 496 for information. The following table describes the available options on the Configuration Search Results page.

Field	Description/Action
Modify this search link	Returns you to the Search For Configuration page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Check Boxes	You can use the left-side check boxes to compare and delete configuration from the NA database. Once you have selected the configurations, click the Actions drop-down menu and click either: • Compare — Opens the Compare Device Configurations page, where you can compare any two configurations. The differences are highlighted for easy reference. You can also deploy configurations from this page. • Delete — Deletes the selected configuration from the NA database. The adjacent Select drop-down menu enables you to select or deselect all of the devices.
Actions	You can select the following actions for each entry in the Configuration Search Results table: • Compare to Previous — The Compare Device Configurations page opens, where you can view this and the previous configurations side by side. The differences are highlighted in different colors to make them easy to read. • View Config — Opens the Device Configuration Detail page, where you can edit and add comments to the selected configuration. You can also deploy the selected configuration from this page. • Diagnostics — Opens the Diagnostics page, where you can view diagnostic information for this configuration.
Search Criteria	Displays the search criteria used in the search. You can: • Save result devices as a new device group — Enter the name of the new group and click Create Group. • Add result devices to existing device group — Select a group from the drop-down menu and click Add. (**Note**: For information on creating a Dynamic Group, refer to "Dynamic Device Groups" on page 142.) • Save the search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. • Email Search Result — Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as a CSV file — Downloads the search results in CSV format. (**Note**: Check the "Include result details" option if you checked the "Configuration Text" option and entered the configuration text you want to find when defining the search criteria on the Search for Configuration page. The configuration text is not included in the CSV file if you do not check the "Include result details" option.)

Searching for Diagnostics

Diagnostic searches provide access to your device diagnostic information based on search criteria you define. Results match all search criteria. The type of information provided by each diagnostic is device-specific.

To search for diagnostics, on the menu bar under Reports select Search For and click Diagnostics. The Search For Diagnostic page opens.

Note: When entering search criteria, your settings are lost if you change to a different page before running the search.

When you are done entering your search criteria and click the Search button, NA returns a list of diagnostics containing all the specified search criteria on the Diagnostics Search Results page. Refer to "Diagnostic Search Results Page Fields" on page 503 for information.

Note: The NA VLAN Data Gathering and the NA Topology Gathering diagnostics are not searchable. Refer to "View Menu Options" on page 203 for more information.

Search For Diagnostic Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the Diagnostics Search Results page to show only the selected information.
Host Name	Select an operator and enter the host name of the device. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the “equals” and “does not equal” operators.)
Device IP	Select an operator and then enter the IP address of the device.
Date	Select the following operators: • Since or Until • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.
Diagnostic Type	Select the type of diagnostic data on which you want to search from the scroll-down menu. To select or deselect multiple types, use Ctrl+click. Diagnostic types include: • NA Device File System • Hardware Information • ICMP Test • Memory Troubleshooting • NA Detect Device Boot • NA Flash Storage Space • NA Interfaces • NA Module Status • NA OSPF Neighbors • NA Port Scan • NA Routing Table • NA Topology Data Gathering **Note**: For detailed information on diagnostics, refer to Diagnostics field on the “View Menu Options” on page 203.

Field	Description/Action
Device Status	Select from the following options for the device: • Active • Inactive • Pre-Production (A pre-production device is a device that is not yet active in the production network. Refer to “Bare Metal Provisioning” on page 118 for information.)
Diagnostic Text	Select an operator (contains or does not contain) and enter a unique portion of the diagnostics you want to search for or exclude from the search results. This field is case-sensitive unless the tips at the top of the page indicate that *all* text field searches are case-insensitive.
Diagnostic Custom Data	Select an operator and enter the unique text that might appear in any of the custom fields that are listed. (**Note**: This section is not displayed if there are no custom fields.)
Device belongs to	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use the Device Selector to select groups. For information on how to use the Device Selector, refer to “Device Selector” on page 144.
Partition	Select a Partition to limit search results to devices in that Partition. The Default Partition (named Default Site) initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Partitions. Refer to “Partitions” on page 158 for detailed information on Partitions.)

Diagnostic Search Results Page Fields

The Diagnostics Search Results page display depends on the search criteria you selected on the Search for Diagnostics page. Refer to "Search For Diagnostic Page Fields" on page 501 for information. The following table describes the available options on the Diagnostic Search Results page.

Option	Description/Action
Modify this search link	Returns you to the Search For Diagnostic page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Check Boxes	You can use the left-side check boxes to select Diagnostics from the NA database. Once you have selected the diagnostics, click the Actions drop-down menu and click: • Compare — Opens the Compare Diagnostics Type page, where you can compare any two diagnostics of the same type. • Delete — Deletes the selected configuration from the NA database. The adjacent Select drop-down menu enables you to select or deselect all of the diagnostics.
Actions	You can select the following actions for each entry in the Diagnostics Search Results table: • View Detail — Enables you to view the details of the diagnostic. • Compare to Previous — Compares this diagnostic to the previous one.
Search Criteria	Displays the search criteria used in the search. You can: • Save as a new device group — Select either "All Result Devices" or "Selected Devices Only," enter the name of the new device group, and click Create Group. • Add to an existing static device group — Select either "All Result Devices" or "Selected Devices Only," select a device group from the drop-down menu, and click Add. • Save search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. Refer to "User & System Reports" on page 599 for information. • Email Search Result - Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as CSV File - Downloads the search results in CSV format.

Searching for Tasks

Task searches enable you to search the NA database for tasks scheduled on your network.

To search for tasks, on the menu bar under Reports select Search For and click Tasks. The Search For Task page opens. Make a selection for any field to be included in the search. Select the check box for each field to be included on the Tasks Search Results page.

When you click the Search button, NA returns a list of tasks containing all the specified search criteria on the Task Search Results page. Refer to "Task Search Results Page Fields" on page 511 for information.

Note: When entering search criteria, your settings are lost if you change to a different page before running the search.

Search For Task Page Fields

All fields are optional.

Field	Description/Action
Task Name	The task name. Select an operator, and then enter a value. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal
Host Name	The host name of the device on which the tasks run. Select an operator, and then enter a value. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)

Field	Description/Action
Device IP	The IP address of the device on which the tasks run. Select an operator, and then enter a value. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal
Scheduled By	The NA user name of the person who scheduled the tasks. Select an operator, and then enter a value. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal
Scheduled Date	The time the tasks are scheduled to run. For one or both rows select Since or Until, and then select a value: • Anytime • Customize (opens the calendar) • Now • 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.
Start Date	The time the tasks actually started. For one or both rows select Since or Until, and then select a value: • Anytime • Customize (opens the calendar) • Now • 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.

Field	Description/Action
Complete Date	The time the tasks completed. For one or both rows select Since or Until, and then select a value: • Anytime • Customize (opens the calendar) • Now • 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.
Duration	The duration (in seconds) of the tasks. This value is the difference between the complete date and the start date. Select an operator, and then enter a value. Operators include: • equals • is less than • is greater than
Task Status	The task status filter. To select or deselect multiple values, use Ctrl+click. Options include: • Pending • Succeeded • Failed • Running • Paused • Draft • Waiting • Duplicate • Skipped • Warning • Requested • Templates
Task Priority	Enter a task priority. Refer to “Scheduling Tasks” on page 280 for information on task scheduling.

Field	Description/Action
Task Type	The task type filter. To select or deselect multiple values, use Ctrl+click. Options include: • Add Device Context • Backup Device Software • Check Policy Compliance • Configure Syslog • Data Pruning • Deduplication • Delete ACLs • Deploy Config • Deploy Passwords • Deploy Remote Agent • Detect Network Devices • Discover Driver • Download Image from Cisco.com • Email Report • Generate Summary Reports • Import • IOS XR Software • OS Analysis • Port Scan • Provision Device • Reboot Device • Remove Device Context • Resolve FQDN • Run Command Script • Run Diagnostics • Run External Application • Run ICMP Test • Synchronize Startup and Running • Take Snapshot • Update Device Software • VLAN Task • Multi-Task Project

Field	Description/Action
Failure Type	The task failure type filter. To select or deselect multiple values, use Ctrl+click. Options include: • Cancelled by user (pending) • Cancelled by user (waiting) • Core stopped • Device unreachable • Incorrect password • Insufficient privileges • No password found • Timed out • Unrecognized device • Unsupported device
Comments	The task comment text. Select an operator, and then enter a value. Operators include: • contains • does not contain
Result	The task result text. Select an operator, and then enter a value. Operators include: • contains • does not contain If the search operator is contains, set the number of context lines around the matching line in the Show context lines around the matching line when displaying text fields field.
Core	The name of the NA core with which the tasks are associated. Select an operator, and then enter a value. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal

Field	Description/Action
Approve By Date	The time the tasks were approved. For one or both rows select Since or Until, and then select a value: • Anytime • Customize (opens the calendar) • Now • 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.
Approval Status	The task approval status filter. To select or deselect multiple values, use Ctrl+click. Options include: • Approved • Draft • Not Applicable • Not Approved • Overridden • Waiting Approval
Device Type	The type of device (for example: router, switch, firewall, VPN, DialUp, DSL_ISDN, or load balancer) on which the tasks run. To select or deselect multiple values, use Ctrl+click. The list of options depends on the devices in the NA inventory.
Exclude Child Tasks	If selected, child tasks are excluded from the search.
Custom Data	Select an operator, and then enter the unique text that might appear in any of the custom fields that are listed. **Note**: This section is not displayed if there are no custom fields.
Show context lines around the matching line when displaying text fields	If the search operator for the Result field is contains, set the number of context lines around the matching line in this field. The default is 3. The maximum is 5. **Note**: This feature can significantly slow performance if there is a large number of results to load.

Field	Description/Action
Device belongs to group	The device group filter. Select an operator, and then select one or more device groups. Operators include: • Any of selected groups (the default) • All of selected groups • None of selected groups For information about how to select device groups, see “Device Selector” on page 144.
Partition	The name of the partition in which the tasks run. Select a partition from the list. **Note**: This field is only displayed if NA uses partitions.

Task Search Results Page Fields

The Tasks Search Results page display depends on the search criteria you selected on the Search for Task page. Refer to "Search For Task Page Fields" on page 504 for information. The following table describes the available options on the Task Search Results page.

Option	Description/Action
Modify this search link	Returns you to the Search For Tasks page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Check Boxes	You can use the left-side check boxes delete tasks from the Task Search Results table. Once you have selected the tasks, click the Actions drop-down menu and click: • Delete — Deletes the selected tasks. The adjacent Select drop-down menu enables you to select or deselect all of the tasks.
Actions	You can select the following actions for each entry in the Tasks Search Results table: • Edit — The Edit Task page opens, where you can edit and rerun a task that is recurring or has not yet occurred. This link appears only when you can edit the task. • Delete — Deletes the task. This link appears only when the task has not yet run. • Pause — Pauses the task. This link appears only when the task has not yet run. • Run Now — Runs the task. This link appears only when the task has not yet run. • Run Again — The Rerun Task page opens, where you can rerun the task. • Detail — The Task Information page opens, where you can view task details. • Cancel — Cancels the task.

Option	Description/Action
Search Criteria	Displays the search criteria used in the search. You can: • Save as a new device group — Select either “All Result Devices” or “Selected Devices Only,” enter the name of the new device group, and click Create Group. • Add to an existing static device group — Select either “All Result Devices” or “Selected Devices Only,” select a device group from the drop-down menu, and click Add. • Save search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. Refer to “User & System Reports” on page 599 for information. • Email Search Result - Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as a CSV file — Downloads the search results in CSV format. (**Note**: Check the “Include result details” option if you checked the “Result” option and entered the task results you want to find when defining the search criteria on the Search for Tasks page. The task results are not included in the CSV file if you do not check the “Include result details” option.)

Searching for Sessions

NA's script execution and management capabilities provide tremendous benefits when it comes to pushing out changes to multiple devices simultaneously. However, for those with little scripting experience, creating command scripts can be difficult. As a result, NA's ScriptMaster enables NA to automatically generate scripts based on Telnet or SSH sessions recorded through the Telnet/SSH Proxy.

You can use session searches to find Telnet/SSH Proxy sessions. In addition, you can configure the Session Search Results page to include session data that appears before and after the matching session data to provide a context for interpreting the results.

Note that there is an Admin Setting that determines whether NA saves just the commands or the full Telnet/SSH command session. Refer to "Telnet/SSH Page Fields" on page 67.

To search for sessions, on the menu bar under Reports, select Search For and click Telnet/SSH Sessions. The Search For Session page opens. When you are finished entering search criteria and click the Search button, NA returns a list of Telnet/SSH sessions containing all the specified search criteria on the Session Search Results page. Refer to "Session Search Results Page Fields" on page 516 for information.

Note: When entering search criteria, your settings are lost if you change to a different page before running the search.

Search For Session Page Fields

Field	Description/Action
Host Name	Select an operator and enter the host name of the device associated with the session. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Device IP	Select an operator and enter the IP address of the device associated with the session.
Device Status	Select from the following options for the device: • Active • Inactive • Pre-Production (A pre-production device is a device that is not yet active in the production network. Refer to "Bare Metal Provisioning" on page 118 for information.)

Field	Description/Action
Created By	Select an operator and enter the login name of the person who might have created a session.
Start Date	Select the following operators: • Since/Until • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.
End Date	Select the following operators: • Since/Until • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.
Status	Select one or more of the following status options: • Failed • Open • Closed
Session Type	Select one of the following options: • Any • Telnet • SSH
Session Data	Select an operator (contains or does not contain) and enter a unique portion of the session you want to find. This field is case-sensitive unless the tips at the top of the page indicate that *all* text field searches are case-insensitive. If the search operator is “contains,” you can provide a value in the <#> context lines box at the bottom of the page. You can include up to five lines above and below the search text in the results. (**Note**: When the number of results to load is large, showing context lines can significantly slow performance.)
Session Custom Data	Select an operator and enter the unique text that might appear in any of the custom fields that are listed. (**Note**: This section is not displayed if there are no custom fields.)
Device belongs to	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use the Device Selector to select groups. For information on how to use the Device Selector, refer to “Device Selector” on page 144.

Field	Description/Action
Partition	Select a Partition to limit search results to devices in that Partition. The Default Partition (named Default Site) initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Partitions. Refer to "Partitions" on page 158 for detailed information on Partitions.)

Session Search Results Page Fields

The Session Search Results page display depends on the search criteria you selected on the Search for Sessions page. Refer to "Search For Session Page Fields" on page 513 for information. The following table describes the available options on the Session Search Results page.

Option	Description/Action
Modify this search link	Returns you to the Search For Sessions page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Actions	You can select the following actions for each entry in the Session Search Results table: • Host Name — Opens the Device Information page, where you can view basic information about the device and its configuration history. • Device IP — Opens the Device Information page, where you can view basic information about the device and its configuration history. • View Full Telnet/SSH Session — Opens the Telnet/SSH Session page, where you can see the commands and system responses for that session. This page includes the Convert to Script links that simplifies creation of a script from commands run during the current session. Refer to "Adding Command Scripts" on page 582 for information. There is also a link to the configuration (if any) created by this session. • View Commands Only — Opens the Telnet/SSH Session page, where you can see just the commands for that session. This page includes the Convert to Script links that simplifies creation of a script from commands run during the current session. There is also a link to the configuration (if any) created by this session.
Search Criteria	Displays the search criteria used in the search. You can: • Save as a new device group — Select either "All Result Devices" or "Selected Devices Only," enter the name of the new device group, and click Create Group. • Add to an existing static device group — Select either "All Result Devices" or "Selected Devices Only," select a device group from the drop-down menu, and click Add. • Save search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. Refer to "User & System Reports" on page 599 for information. • Email Search Result - Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as a CSV file — Downloads the search results in CSV format. (**Note**: Check the "Include result details" option if you checked the "Session Data" option and entered the session data you want to find when defining the search criteria on the Search for Session page. The session data is not included in the CSV file if you do not check the "Include result details" option.)

Searching for Events

You can search for system and user events, such as a device access failure. Refer to "Event Descriptions" on page 520 for a description of NA events.

To search for events, on the menu bar under Reports, select Search For and click Events. The Search For Events page opens. When you are finished entering search criteria and click the Search button, NA returns a list of events containing all the specified search criteria on the Event Search Results page. Refer to "Event Search Results Page Fields" on page 519 for information.

Note: When entering search criteria, your settings are lost if you change to a different page before running the search.

Search For Events Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the Event Search Results page to show only the selected information.
Date	Select the following operators: • Since/Until • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.
Summary	Select the name of one or more events. Use Ctrl+click to select/deselect additional events. Refer to "Event Descriptions" on page 520 for detailed information on each event.
Added By	Select an operator and provide the login name of the person who created the event.
Importance	Select one or more of the following options: • Informational — Events that typically do not require a response. • Low — Events that may require a response as time permits. • Medium — Events that require a timely response, typically within 72 hours. • High — Events that require an urgent response, typically within 24 hours. • Critical — Events that require an immediate response.

Field	Description/Action
Host Name	Select an operator and enter the host name of the device associated with these events. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Device IP	Select an operator and enter the IP address of the device associated with these events.
Description	Select an operator (contains or does not contain) and enter the unique text from the event you are searching for. This field is case-sensitive unless the tips at the top of the page indicate that *all* text field searches are case-insensitive. To show the text in the results page, you can include up to five lines above and below the search text in the results. (**Note**: When the number of results to load is large, showing context lines can significantly slow performance.)
Device belongs to group	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use the Device Selector to select groups. For information on how to use the Device Selector, refer to "Device Selector" on page 144.
Partition	Select a Partition to limit search results to devices in that Partition. The Default Partition (named Default Site) initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Partitions. Refer to "Partitions" on page 158 for detailed information on Partitions.)

Event Search Results Page Fields

The Event Search Results page display depends on the search criteria you selected on the Search for Events page. Refer to "Search For Events Page Fields" on page 517 for information. The following table describes the available options on the Event Search Results page.

Field	Description/Action
Modify this search link	Returns you to the Search For Events page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Check Boxes	The check boxes for each event enable you to delete events. Once you have selected the events, click the Actions drop-down menu and click: • Delete — Deletes the selected events. The adjacent Select drop-down menu enables you to select or deselect all of the tasks.
Actions	You can select the following actions for each entry in the Events Search Results table: • Summary — Opens the Event Detail page, where you can view the detailed result of this event. • Host Name — Opens the Device Details page, where you can view basic information about the device and its configuration history.
Search Criteria	Displays the search criteria used in the search. You can: • Save as a new device group — Select either "All Result Devices" or "Selected Devices Only," enter the name of the new device group, and click Create Group. • Add to an existing static device group — Select either "All Result Devices" or "Selected Devices Only," select a device group from the drop-down menu, and click Add. • Save search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. Refer to "User & System Reports" on page 599 for information. • Email Search Result - Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as a CSV file — Downloads the search results in CSV format. (**Note**: Check the "Include result details" option if you checked the "Description" option and entered the event description text you want to find when defining the search criteria on the Search for Events page. The event description text is not included in the CSV file if you do not check the "Include result details" option.)

Event Descriptions

The following table describes the NA events. The events are listed in alphabetical order.

Event	Description
Approval Denied	A user has denied an approval request.
Approval Granted	A user has approved a task.
Approval No Longer Required	A task approval is no longer required.
Approval Override	A user has overridden the approval of a task allowing the task to run without approval.
Approval Request	A user has created a task that requires approval before it can run.
Approval Task Changed	A user has made a change to a task that requires approval before it can run.
Approval Task Deleted	A user has deleted a task that was earmarked for approval.
Approval Task Timeout	A task was not approved in the time allotted.
Command Authorization Error	A user tried to run a command that he/she is not authorized to use.
Command Script Modified	A command script has been modified.
Concurrent Telnet/SSH Session Override	A user ignored the restriction on simultaneous logins. The user logged-in to a device via the Proxy despite another user's prior login.
Device Access Failure	NA cannot access a device. This could be due to a bad password or there was no route to the host.
Device Added	A user added a device.
Device Booted	A device was rebooted.
Device Command Script Completed Successfully	A device command script succeeded.
Device Command Script Failed	A device command script failed.
Device Configuration Change	NA detected a configuration change while running a Snapshot task.
Device Configuration Change - No User	NA detected a configuration change by an unknown user.
Device Configuration Deployment	NA successfully deployed a configuration to a device.
Device Configuration Deployment Failure	NA failed to deploy a configuration to a device.
Device Context Add Failed	A device context addition failed.
Device Context Added	A device context was successfully added.
Device Context Remove Failed	A device context remove failed.
Device Context Removed	A device context was successfully removed.

Event	Description
Device Data Failure	NA failed to save a configuration or diagnostic output to the database.
Device Deleted	A user permanently removed a device.
Device Diagnostic Changed	The results of a diagnostic differ from the previous results.
Device Diagnostic Completed Successfully	A device diagnostic succeeded.
Device Diagnostic Failed	A device diagnostic failed.
Device Edited	A user modified a device's information.
Device Flash Storage Running Low	A device’s flash storage is running low.
Device Group Added	A user has added a group.
Device Group Deleted	A user has deleted a group.
Device Group Modified	A user modified a device group.
Device Inaccessible	A device is inaccessible.
Device Managed	A user marked a device as Active.
Device Missing From Import	When the Import task is run periodically and given a file of devices to import, this event occurs when a device was included in the file the last time the import occurred, but is no longer included in the file during the current import.
Device Password Change	A user deployed a password change.
Device Password Change Failure	NA failed to deploy a device password change.
Device Permissions - Modified	A device was added to or removed from a group, which changed permissions such that users can modify the device.
Device Permissions - New Device	Someone added a new device to a device group, changing the permissions for users associated with that device group.
Device Port Duplex Mismatch Detected	A device port duplex mismatch was detected.
Device Provision Failed	A device was not successfully provisioned.
Device Provision Succeeded	A device successfully provisioned.
Device Relationship Added	A device relationship was successfully added.
Device Relationship Deleted	A device relationship was successfully deleted.
Device Relationship Modified	A device relationship was successfully modified.
Device Reload Failed	A device reload failed.
Device Reloaded	A device was successfully reloaded.
Device Reservation Conflict	There was a device reservation conflict.

Event	Description
Device Snapshot	NA checked a device for a configuration change.
Device Software Change	NA detected a new OS version on a device (for example: from IOS 11 to IOS 12).
Device Startup/Running Config Difference	NA detected a difference between the Startup and Running configurations.
Device Template Added	A device template was successfully added.
Device Template Deleted	A device template was successfully deleted.
Device Template Edited	A device template was successfully edited.
Device Unmanaged	A user marked a device as Inactive. Imported devices can also be Inactive if unreachable for a certain time of period.
Diagnostic Modified	A user has modified a diagnostic.
Distributed System — Abnormal Shutdown of Core	A running NA core detected and responded to the unexpected shutdown of another NA core in the Horizontal Scalability environment.
Distributed System — Broken Replication Job	NA detected a broken replication job.
Distributed System — Data Synchronization Delay Warning	NA detected a data synchronization delay warning.
Distributed System — Deferred LOBs Exceed Threshold	NA detects deferred LOBs that exceeded the threshold.
Distributed System — Deferred Transactions Exceed Threshold	NA detects deferred transactions that exceeded the threshold.
Distributed System — Device Software Transfer Error	NA detected a device software transfer error.
Distributed System — Fixed Replication Job	NA detected a fixed replication job.
Distributed System — Normal Shutdown of Core	An NA core communicated its transition before shutting down.
Distributed System — Processed Normal Shutdown of Core	A running NA core responded to the normal shutdown of another NA core in the Horizontal Scalability environment.
Distributed System — Replication Errors	NA detected replication errors.
Distributed System — RMI Error	NA detected a RMI error.
Distributed System — Stopped Merge Agent Job	NA detected a stopped merge agent job.
Distributed System — Time Synchronization Warning	NA detected a time synchronization warning.

Event	Description
Distributed System — Undeletable Anomalous Generations	NA detected undeletable anomalous generations.
Distributed System — Uniqueness Conflict	NA detected a uniqueness conflict.
Driver Discovery Failure	NA detected a failed driver discovery.
Driver Discovery Success	NA detected a successful driver discovery.
Driver Load Error	NA detected a driver load error.
Duplicate Device Detected	NA detected a duplicate device.
Dynamic Group Update Error	NA detected a device group update error.
Email Report Saved	A user has saved an email report.
External Directory Server Authentication Error	NA could not connect to an external LDAP authentication server.
Last Used Device Password Changed	The password last used for access to a device was changed.
License Almost Exceeded	The devices exceed 90% of the total number of licensed nodes.
License Almost Expired	Your NA license expires soon (date-based licenses only).
License Exceeded	The devices exceed the total number of licensed nodes. NA allows a 20% excess.
License Expired	Your license has expired. NA will no longer allow logins, but will continue to take scheduled snapshots and record changes.
Module Added	Someone added a module/blade/card to a device.
Module Changed	Someone changed the attributes of a module/blade/card installed in a device.
Module Removed	Someone removed a module/blade/card from a device.
Monitor Error	A server monitor failed to run.
Monitor Okay	A server monitor ran successfully.
Pending Task Deleted	A user deleted a scheduled task before it ran.
Policy Added	A user has added a new configuration policy.
Policy Changed	A user has changed a configuration policy.
Policy Non-Compliance	A configuration change violated a policy rule.
Policy Pattern Timeout	A policy pattern took more than 30 seconds to match.
Policy Rule Added	A user has added a new configuration rule.
Policy Rule Changed	A user has changed a configuration rule.

Event	Description
Reserved Device Configuration Changed	A user has changed the device configuration on a reserved device.
Scheduled for Deploy Configuration Edited	A user modified a configuration that was scheduled to be deployed.
Scheduled for Deploy Password Modified	A new password was deployed, and there is another Password Deploy task scheduled. This indicates that the new password that was just deployed will be changed again (when the pending Password Deploy task executes).
Security Alert	NA has detected a security alert.
Server Startup	The NA Management Engine was started.
Session Data Captured	The Proxy saved a connect session to the database.
Software Update Failed	NA failed to update the OS software on a device.
Software Update Succeeded	NA successfully updated the OS software on a device.
Software Vulnerability Detected	If you setup a software level set to “Security Risk,” when NA snapshots devices and detects an OS version that is tagged as a “Security Risk,” this event is generated.
Summary Reports Generated	A user has generated Summary reports.
Task Completed	A task has completed.
Task Started	A task has started.
Ticket Created	When using the HP Remedy AR System Connector (or any of the HP Connectors that interact with a 3rd party Ticketing systems), this event indicates that NA created a ticket in that 3rd party Ticketing system.
User Added	A user has been added.
User Authentication Error	A user entered an incorrect password when logging into NA.
User Authentication Error Lockout	A user is locked out due to too many consecutive failed login attempts.
User Deleted	A user has been deleted
User Disabled	A user record was edited and the user’s status changes from Enabled to Disabled.
User Enabled	A user record was edited and the user’s status changes from Disabled to Enabled.
User Login	A user logged-in to NA.
User Logout	A user has logged-out of NA.
User Message	A user created a message by clicking the New Message link.
User Permission Changed	A user’s permission has been changed.

Searching for Users

You can use the Search for Users page to search for users by first name, last name, email address, and/or AAA user name. To search for users, on the menu bar under Reports select Search For and click Users. The Search For Users page opens.

When you click the Search button, NA returns a list of events containing all the specified search criteria on the User Search Results page. Refer to "User Search Results Page" on page 526 for information.

Search For Users Page

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the User Search Results page to show only the selected information.
First Name	Select an operator and enter the user's first name. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal
Last Name	Select an operator and enter the user's last name.
User Name	Select an operator and enter the user's username. You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Email Address	Select an operator and enter the user's email address.
AAA User Name	Select an operator and enter the user's AAA username.
Comments	Select an operator (contains or does not contain) and then enter the comment text you want to find.
Member of User Group	Select the user group of which the user(s) are a member.
User Custom Data	Select an operator and enter user custom service data.
Partition	Select a Partition to limit search results to devices in that Partition. The Default Partition (named Default Site) initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Partitions. Refer to "Partitions" on page 158 for detailed information on Partitions.)

User Search Results Page

The User Search Results page displays the search criteria you selected on the Search for Users page. Refer to "Search For Users Page" on page 525 for information.

Field	Description/Action
Modify this search link	Returns you to the Search For Events page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Actions	You can select the following actions for each entry in the Tasks Search Results table: • Edit — Open the My Profile page, where you can edit the user's profile. Refer to "My Profile Page Fields" on page 262 for information. • Delete — Enables you to delete the user if you have the proper permissions. Otherwise, the option is greyed out. • Permissions — Opens the My Permissions page, where you can edit the user's permissions. Refer to "My Permissions Page Fields" on page 266 for information. • Config Changes — Opens the Config Search Results, where you can view configuration changes made by the user.
Search Criteria	Displays the search criteria used in the search. You can: • Save search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. Refer to "User & System Reports" on page 599 for information. • Email Search Result - Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as CSV File - Downloads the search results in CSV format.

Searching for ACLs

Access Control Lists (ACLs) are part of the configuration on most devices. They filter network traffic by controlling whether routed packets are accepted or blocked at the router's interfaces. In general, an ACL is a collection of statements. Each statement defines a pattern that would be found in an IP packet. ACLs are often used to restrict the contents of routing updates and to provide network security.

NA retrieves configuration information from devices and extracts the ACL statements from the configuration. NA then stores the ACLs independent of the configuration. As a result, you can:

- View the current ACLs on a device and compare them against the previous ACLs.
- Add comments to an ACL.
- Modify/create an ACL and deploy it back to the device.

For information on modifying and/or creating an ACL, refer to "Creating ACLs" on page 690.

To search for ACLs, on the menu bar under Reports, select Search For and click ACLs. The Search For ACLs page opens.

Search For ACLs Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the ACL Search Results page to show only the selected information.
Host Name	Select an operator and enter the host name of the device associated with the session. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Device IP	Select an operator and enter the device's IP address.
ACL ID	Select an operator and enter the ACL's ID. The ACL ID is a number or name based on the device ACL list, while the ACL Handle is a descriptive name or value assigned by the user. By default, the ACL ID and ACL Handle are the same until the user defines the ACL Handle.
ACL Handle	Select an operator and enter the ACL's Handle. The ACL Handle is a descriptive name or value assigned by the user. By default, the ACL ID and ACL Handle are the same until the user defines the ACL Handle.
ACL Type	Select an operator and enter the type of ACL, for example: "extended." Keep in mind that ACL types are driver dependent.
ACL Configuration	Select an operator, either contains or does not contain, and enter any configuration commands that define the ACL. This field is case-sensitive unless the tips at the top of the page indicate that *all* text field searches are case-insensitive. If the search operator is "contains," you can provide a value in the <#> context lines box at the bottom of the page. You can include up to five lines above and below the search text in the results. (**Note**: When the number of results to load is large, showing context lines can significantly slow performance.)
ACL Application	Select an operator, either contains or does not contain, and enter the entity that is using the ACL. For example, if an ACL is applied to an interface, the interface is an application of the ACL. This field is case-sensitive unless the tips at the top of the page indicate that *all* text field searches are case-insensitive.
Search Scope	If checked, search results will be limited to those ACLs that are currently configured on all devices. If unchecked, the search results will contain both current and historical ACLs.

Field	Description/Action
Comments	Select an operator, either contains or does not contain, and enter any ACL comments. This field is case-sensitive unless the tips at the top of the page indicate that *all* text field searches are case-insensitive.
Changed By	Select an operator and enter the name of the user that last changed the ACL.
Last Modified	Select the following operators: • Since or Until • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.
Device belongs to group	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use the Device Selector to select groups. For information on how to use the Device Selector, refer to "Device Selector" on page 144.
Partition	Select a Partition to limit search results to devices in that Partition. The Default Partition (named Default Site) initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Partitions. Refer to "Partitions" on page 158 for detailed information on Partitions.)

When you click the Search button, NA returns a list of ACLs containing all the specified search criteria on the ACL Search Results page. Refer to "ACL Search Results Page Fields" on page 530 for information.

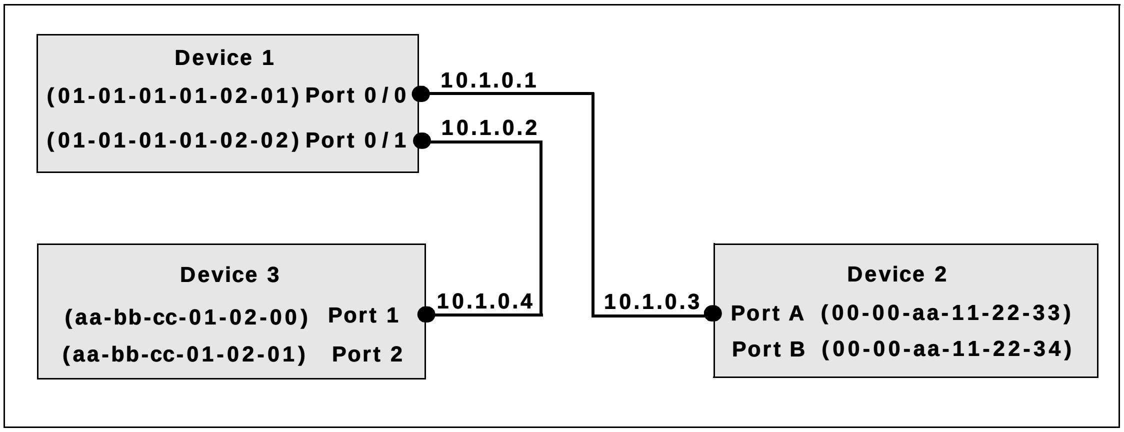
ACL Search Results Page Fields

The ALC Search Results page display on the search criteria you selected on the Search for ACLs page. Refer to “Search For ACLs Page Fields” on page 528 for information. The following table describes the available options on the ACLs Search Results page.

Option	Description/Action
Modify this search link	Returns you to the Search For ACLs page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Check Boxes	The check boxes for each ACL enable you to compare two ACLs. Once you have selected the ACLs, select the Actions drop-down menu and click: • Compare — Opens the Compare ACL page, where you can compare any two ACLs. The differences are highlighted for easy reference. You have the option of displaying differences with context, showing full text, or show UNIX-style differences. The adjacent Select drop-down menu enables you to select or deselect all of the ACLs.
Actions	You can select the following actions for each entry in the ACL Search Results table: • Edit ACL — Opens the Edit ACL page, where you can edit the ACL. Refer to “Deleting ACLs” on page 697 for information. • View ACL — Opens the View ACL page, where you can view the ACL. Refer to “Viewing ACLs” on page 685 for information. • ACL History — Opens ACL History page, where you can edit and view the ACL.
Search Criteria	Displays the search criteria used in the search. You can: • Set handle for selected ACLs — Enter an ACL handle. The ACL Handle is a descriptive name or value assigned by the user. • Save search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. Refer to “User & System Reports” on page 599 for information. • Email Search Result - Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as CSV File - Downloads the search results in CSV format.

Searching for MAC Addresses

MAC addresses are unique addresses that identify ports on a device. MAC addresses are also known as BIAs (Burned-in Addresses), hardware addresses, and physical addresses. NA gathers information about which MAC addresses are assigned to ports on devices and which MAC addresses are visible from those ports. The following figure illustrates the relationship between MAC addresses, IP addresses, and ports.


Device 1
(01-01-01-01-02-01) Port 0/0
(01-01-01-01-02-02) Port 0/1
10.1.0.1
10.1.0.2
Device 3
(aa-bb-cc-01-02-00) Port 1
(aa-bb-cc-01-02-01) Port 2
10.1.0.4
10.1.0.3
Device 2
Port A (00-00-aa-11-22-33)
Port B (00-00-aa-11-22-34)

To search for MAC Addresses, on the menu bar under Reports, select Search For and click MAC addresses. The Search For MAC Address page opens. After you enter your search criteria and click the Search button, NA returns a list of MAC addresses containing all the specified search criteria on the MAC Address Search Results page. Refer to "MAC Address Search Results Page Fields" on page 534 for information.

Search For MAC Address Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the MAC Address Search Results page to show only the selected information.
Host Name	Select an operator and enter the host name of the device. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Device IP	Select an operator and enter the IP address of the device.
Port Name	Select an operator and enter the device port name. The port name is the name of the actual port on the device. For example: Ethernet0/1.
Port Description	Select an operator and enter a description of the port.
Address	Select an operator and enter a MAC address pattern on which to search.
Address Type	Select one of the following options: • All addresses (the default) • Seen from port — Display only those MAC addresses that are connected to the device/port (i.e., those MAC address types external to the device/port, but visible to it). • Address of port — Display only those MAC addresses that are internal to the device (i.e., the MAC addresses that are assigned to ports on the device). **Note**: The "Limit search to MAC addresses no longer seen" check box enables you to limit the search results to only those MAC addresses that are no longer seen in the latest data capture.
Search Scope	If checked, the search is limited to MAC addresses no longer seen.
VLAN	Select an operator and enter the port's VLAN name. The VLAN name is the name of the VLAN, for example VLAN2 or VLAN3, on which to limit the search.
Associated IP	Select an operator and enter an IP address associated with the MAC you are searching for.

Field	Description/Action
Device belongs to group	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use the Device Selector to select groups. For information on how to use the Device Selector, refer to "Device Selector" on page 144.
Partition	Select a Partition to limit search results to devices in that Partition. The Default Partition (named Default Site) initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Partitions. Refer to "Partitions" on page 158 for detailed information on Partitions.)

MAC Address Search Results Page Fields

The MAC Address Search Results page displays the search criteria you selected on the Search For MAC Address page. Refer to "Search For MAC Address Page Fields" on page 532 for information.

Option	Description/Action
Modify this search link	Returns you to the Search For MAC Address page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Actions	You can select the following action for each MAC address: • View Details — Opens the MAC Address Detail page, where you can view details on the following information: Device, Device Port, MAC address, Type, First Seen, and Last Updated. • View IP - Opens the IP Address Detail page that is cross-referenced with this MAC address. This option is only available on "Seen from Port" records. Cross-referencing means that when NA gathers data, the IP address and MAC address were indicated as coming from the same source.
Search Criteria	Displays the search criteria used in the search. You can: • Save as a new device group — Select either "All Result Devices" or "Selected Devices Only," enter the name of the new device group, and click Create Group. • Add to an existing static device group — Select either "All Result Devices" or "Selected Devices Only," select a device group from the drop-down menu, and click Add. • Save search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. Refer to "User & System Reports" on page 599 for information. • Email Search Result - Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as CSV File - Downloads the search results in CSV format.

Searching for IP Addresses

An IP address (Internet Protocol address) is a unique numerical address for network devices. Any participating network device, such as a router, switch, firewall, and so on has their own unique IP address. Currently, NA supports:

- IPv4 — IPv4 supports 32-bit and 64-bit addresses in octet notation
- IPv6 — IPv6 supports 128-bit addresses in octet notation (For detailed information on IPv6 support, see the *NA Installation and Upgrade Guide*.)

To search for IP addresses, on the menu bar under Reports, select Search For and click IP Addresses. The Search For IP Addresses page opens. When you are finished entering search criteria, click the Search button. NA returns a list of IP addresses containing all the specified search criteria on the IP Address Search Results page.

Note: When entering search criteria, your settings are lost if you change to a different page before running the search.

Search For IP Address Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the IP Addresses Search Results page to show only the selected information.
Host Name	Select an operator and enter the host name of the device associated with the session. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the “equals” and “does not equal” operators.)
Device IP	Select an operator and enter the IP address of the device, for example: IPv4: 10.255.?.255, 192.*, 172.16.30.1 IPv6: aff:38:?:10, fc00:c0a8:*, ::1
Port Name	Select an operator and enter the device port name. The port name is the name of the actual port on the device. For example: Ethernet0/1.
Port Description	Select an operator and enter a description of the port.
Address	Select an operator and enter a IP address pattern on which to search, for example: IPv4: 10.255.?.255, 192.*, 172.16.30.1 IPv6: aff:38:?:10, fc00:c0a8:*, ::1

Field	Description/Action
Address Type	Select one of the following options: • All addresses (the default) • Seen from port — Display only those IP addresses that are connected to the device/port (i.e., those IP address types external to the device/port, but visible to it). • Address of port — Display only those IP addresses that are internal to the device (i.e., the IP addresses that are assigned to ports on the device). **Note**: The "Limit search to IP addresses no longer seen" check box enables you to limit the search results to only those IP addresses that are no longer seen in the latest data capture.
Search Scope	If checked, the search is limited to IP addresses no longer seen.
VLAN	Select an operator and enter the port's VLAN name. The VLAN name is the name of the VLAN, for example VLAN2 or VLAN3, on which to limit the search.
Associated MAC	Select an operator and enter an associated MAC address.
Device belongs to group	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use the Device Selector to select groups. For information on how to use the Device Selector, refer to "Device Selector" on page 144.
Partition	Select a Partition to limit search results to devices in that Partition. The Default Partition (named Partition) initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Partitions. Refer to "Partitions" on page 158 for detailed information on Partitions.)

IP Address Search Results Page Fields

The IP Address Search Results page displays the search criteria you selected on the Search For IPs page. Refer to “Search For IP Address Page Fields” on page 535 for information.

Option	Description/Action
Modify this search link	Returns you to the Search For IP Address page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Actions	You can select the following action for each MAC address: • View Details — Opens the IP Address Details page, where you can view details on the following information: Device, Device Port, IP address, Type, First Seen, and Last Updated. • View IP - Opens the IP Address detail page that is cross-referenced with this IP address. This option is only available on “Seen from Port” records. Cross-referencing means that when NA gathers data, the IP address and MAC address were indicated as coming from the same source.
Search Criteria	Displays the search criteria used in the search. You can: • Save as a new device group — Select either “All Result Devices” or “Selected Devices Only,” enter the name of the new device group, and click Create Group. • Add to an existing static device group — Select either “All Result Devices” or “Selected Devices Only,” select a device group from the drop-down menu, and click Add. • Save search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. Refer to “User & System Reports” on page 599 for information. • Email Search Result - Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as CSV File - Downloads the search results in CSV format.

Searching for VLANs

VLANs (Virtual Local Area Networks) are conglomerations of ports that act as a single broadcast domain. VLANs operate at Layer 2 (the Data Link layer). NA gathers information about what VLANs are defined on a device and what VLAN each port is assigned to. For detailed information on VLANs, refer to "Virtual Local Area Networks (VLANs)" on page 215.

To search for VLANs, on the menu bar under Reports, select Search For and click VLAN. The Search For VLAN page opens. When you are finished entering search criteria, click the Search button. NA returns a list of VLANs containing all the specified search criteria on the VLAN Search Results page.

Note: When entering search criteria, your settings are lost if you change to a different page before running the search.

Search For VLAN Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the VLANs Search Results page to show only the selected information.
Host Name	Select an operator and enter the host name of the device associated with the session. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Device IP	Select an operator and enter the IP address of the device.
VLAN ID	Select an operator and enter the VLAN's ID. The VLAN ID identifies the VLAN using a 12-bit field in the VLAN's tag. Refer to "Virtual Local Area Networks (VLANs)" on page 215 for detailed information on VLANs.
VLAN Name	Select an operator and enter the VLAN name.
VLAN Type	Select an operator and enter the VLAN type.
VLAN Description	Select an operator and enter the VLAN's description.
Private VLAN	Select an operator and enter the private VLAN description.

Field	Description/Action
Device belongs to group	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use the Device Selector to select groups. For information on how to use the Device Selector, refer to "Device Selector" on page 144.
Partition	Select a Partition to limit search results to devices in that Partition. The Default Partition (named Default Site) initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Partitions. Refer to "Partitions" on page 158 for detailed information on Partitions.)

VLAN Search Results Page Fields

The VLAN Search Results page displays the search criteria you selected on the Search For VLAN page. Refer to "Search For VLAN Page Fields" on page 538 for information.

Option	**Description/Action**
Modify this search link	Returns you to the Search For VLANs page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Actions	You can select the following action for each VLAN: • View Details — Opens the VLAN Detail page, where you can view details about the search with links to the Device and Interface Detail pages. Refer to "VLAN Detail Page Fields" on page 219 for information. • Edit — Opens the Edit VLAN Detail page. Refer to "Creating and Editing VLANs" on page 218 for information. • Delete — Opens a dialog box, where you can confirm that you want to delete the VLAN.
Search Criteria	Displays the search criteria used in the search. You can: • Save as a new device group — Select either "All Result Devices" or "Selected Devices Only," enter the name of the new device group, and click Create Group. • Add to an existing static device group — Select either "All Result Devices" or "Selected Devices Only," select a device group from the drop-down menu, and click Add. • Save search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. Refer to "User & System Reports" on page 599 for information. • Email Search Result - Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as CSV File - Downloads the search results in CSV format.

Searching for Device Templates

Device templates enable you to define configurations, OS/file specifications, and other device-specific information that can then be applied to existing devices. Device templates also have the ability to support certain device operations, such as policy checking, without needing an actual device to test against. Refer to "Device Templates" on page 120 for information.

To search for device templates, on the menu bar under Reports, select Search For and click Device Templates. The Search For Device Template page opens. When you are finished entering search criteria, click the Search button. NA returns a list of device templates containing all the specified search criteria on the Device Templates Search Results page.

Note: When entering search criteria, your settings are lost if you change to a different page before running the search.

Search For Device Template Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the Device Template Search Results page to show only the selected information.
Template Name	Select an operator and enter the name of the device template. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the "equals" and "does not equal" operators.)
Device Vendor	Select an operator and enter the device vendor.
Device Model	Select an operator and enter the device model.
Driver Name	Select a driver from the list.
Device Description	Select an operator and enter a description.
Comments	Select an operator and enter comments. This field is case-sensitive unless the tips at the top of the page indicate that *all* text field searches are case-insensitive.

Field	Description/Action
Configuration Text	Select an operator, and then enter a unique portion of the device configuration on which to search. • The "contains" and "does not contain" operators support regular expressions, including the ? and * wildcards. These searches are case-sensitive unless the tips at the top of the page indicate that *all* text field searches are case-insensitive. • The "contains (full text)" and "does not contain (full text)" operators support the * wildcard only. For more information, see "Using the Full-Text Search Functionality" on page 472. These searches are always case-insensitive. (**Note**: These operators require that full-text search is enabled for the database.) • IPv6 address shorthand notation (double colon) cannot be used in combination with wildcards. If the search operator is "contains" or "contains (full text)," you can provide a value in the "Show <#> context lines around the matched line when displaying Current Configuration" check box at the bottom of the page. You can include up to five lines above and below the search text in the results page. The default value is three. (**Note**: When the number of results to load is large, showing context lines can significantly slow performance.)
Create Date	Select the following operators: • Since or Until • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.
Device Custom data	Select an operator and enter device custom data.
Partition	Select a Partition to limit search results to devices in that Partition. The Default Partition (named Default Site) initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Partitions. Refer to "Partitions" on page 158 for detailed information on Partitions.)

Device Templates Search Results Page Fields

The Device Search Results page displays the search criteria you selected on the Search For Device Template page. Refer to "Searching for Device Templates" on page 541 for information.

Option	Description/Action
Modify this search link	Returns you to the Search For Device Template page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Actions	You can select the following action for each device template: • Edit — Opens the Edit Device Template page, where you can edit information about this Device Template. Refer to "Device Template Page Fields" on page 120. • View Config — Opens the Current Configuration page, where you can edit and add comments to the selected configuration.
Search Criteria	Displays the search criteria used in the search. You can: • Save as a new device group — Select either "All Result Devices" or "Selected Devices Only," enter the name of the new device group, and click Create Group. • Add to an existing static device group — Select either "All Result Devices" or "Selected Devices Only," select a device group from the drop-down menu, and click Add. • Save search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. Refer to "User & System Reports" on page 599 for information. • Email Search Result - Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as CSV File - Downloads the search results in CSV format.

SingleSearch

To search for device change events, on the menu bar under Reports, click SingleSearch. The SingleSearch Page opens. When you click the Search button, NA returns a list of events containing all the specified search criteria you specify on this page on the SingleSearch Results page. Refer to "SingleSearch Results Page Fields" on page 546.

SingleSearch Page Fields

Field	Description/Action
Check boxes	Use the left-side check boxes to customize the Events Search Results page to show only the selected information.
Date	Select the following operators: • Since or Until • Anytime, Customize (opens the calendar), Now, or 1 hour ago to 1 year ago **Note**: Clicking the calendar icon opens the calendar, where you can select a date and time.
Summary	Select the name of one or more events. Use Ctrl+click to select/deselect additional events. Refer to "Event Descriptions" on page 520 for detailed information on each event.
Added By	Select an operator and provide the login name of the person who created the event. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal
Importance	Select one or more Importance level. Options include: • Informational — Events that typically do not require a response. • Low — Events that may require a response as time permits. • Medium — Events that require a timely response, typically within 72 hours. • High — Events that require an urgent response, typically within 24 hours. • Critical — Events that require an immediate response.

Field	Description/Action
Host Name	Select an operator and enter the host name of the device associated with these events. Operators include: • Contains • Does not contain • Matches • Equals • Does not equal You can use wildcard characters. The ? stands for any one character in that position, while the * stands for any number of characters in that position, for example: usa-ny-ny-*, 10.0.*.2, and ?jones. (**Note**: Wildcards do not work with the “equals” and “does not equal” operators.)
Device IP	Select an operator (see above) and enter the IP address of the device associated with these events.
Description	Select an operator (contains or does not contain) and enter the unique text from the event for which you are searching. To show the context lines around the matched line when displaying the event description, check Show and enter the number of lines. Three is the default value.
Device Belongs to group	Select an operator (Any of the selected groups, All of the selected groups, or None of the selected groups) and select one or more groups from the scroll-down list.
Partition	Select a Partition to limit search results to devices in that Partition. The Default Partition (named Default Site) initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Partitions. Refer to “Partitions” on page 158 for detailed information on Partitions.)

SingleSearch Results Page Fields

The SingleSearch Results page display depends on the search criteria you selected on the Search for Single Search. Refer to "SingleSearch Page Fields" on page 544 for information. The following table describes the available options on the SingleSearch Results page.

Field	Description/Action
Modify this search link	Returns you to the SingleSearch page, where you can edit your search criteria and run the search again.
View Search Criteria link	Scrolls down to the Search Criteria information.
Check Boxes	The check boxes for each event enables you to delete events. Once you have selected the events, click the Actions drop-down menu and click: • Delete — Deletes the selected events. The adjacent Select drop-down menu enables you to select or deselect all of the tasks.
Search Criteria	Displays the search criteria used in the search. You can: • Save as a new device group — Select either "All Result Devices" or "Selected Devices Only," enter the name of the new device group, and click Create Group. • Add to an existing static device group — Select either "All Result Devices" or "Selected Devices Only," select a device group from the drop-down menu, and click Add. • Save search as a user report — Enter the name of the user report and click Save. You can view User reports from the User & System Reports page. Refer to "User & System Reports" on page 599 for information. • Email Search Result - Enter the email address to send the search results to and click Send. Be sure to separate multiple addresses with a comma. • View Search Result as CSV File - Downloads the search results in CSV format.

Advanced Search

The Advanced Search page enables you to:

- Create a Boolean expression using the AND and OR operators to filter searches. You can use parenthesis in the Boolean expressions to refine the search.

  Note: This tool does not support the use of regular expresssions.

- Configure searches using one or more search criteria, for example IP address, Domain Name, and Policy Compliance.
- Limit a search by device group.
- Customize the output of the Advanced Search Results page.

To open the Advanced Search page, on the menu bar under Reports, click Advanced Search. When you click the Search button, NA returns the search criteria you specified.

Advanced Search Page Fields

Field	Description/Action
Search For	Select one of the following options from the drop-down menu: • ACL • Compliance • Configuration • Device • Diagnostic • Event • Interface • Module • Session • Task
Search Criteria Each time you select a search criterion, it is displayed in the Search Criteria section, where you can then select an operator, such as Contains, Matches, or Equals, and then enter the information on which to search. If you want to delete a defined criterion, click the X next to the search criterion index letter.	
Add Criteria	Select one or more search criteria from the drop-down menu, for example: • Host Name • Device IP • Domain Name • Device Status • Policy Compliance

Field	Description/Action
Boolean Expression	
Expression	By default, the defined criteria index letters are displayed with the Boolean 'and' expression. For example, if you defined three search criteria, the expression would look like *A and B and C*. You can edit the Boolean expression as needed. Click the Reset Expression button to reset the expression to the default. (**Note**: The maximum number of criteria is 10.)
Limit search by device group	
Device belongs to group	Select one of the following operators from the drop-down menu and then select one or more device groups: • Any of selected groups (the default) • All of selected groups • None of selected groups **Note**: Use the Device Selector to select groups. For information on how to use the Device Selector, refer to "Device Selector" on page 144.
Partition	Select a Partition. The default Partition (named Default Site) initially includes all of Inventory. (**Note**: This field is only displayed if you have configured one or more Partitions. Refer to "Partitions" on page 158 for detailed information on Partitions.)
Customize Output	
Select fields to be included in search results	Select the fields to be included in the Advanced Search Results page. To select multiple fields, click the first field, then Ctrl+click to select/deselect additional fields.
Sort results by	Select the search criterion from the drop-down menu for which you want to sort the results of the search. You can specify Ascending (the default) or Descending.
Display results in groups of	Enter the number of items you want displayed on the Advanced Search Results page. The default 25.
Show <#> context lines around the matching line when displaying text fields	When displaying text fields on the Advanced Search Results page, enter the number of lines around the matching line to be displayed. The default is 3.

Sample Advanced Search

The following advanced search assumes that you have two data centers under management. One data center is located on the New York and the other in California. The search informs you of all the Cisco devices that do not have the proper timezone set for either of the data centers.

1. Log into NA.
2. From the main menu bar under Reports, click Advanced Search. The Advanced Search page open.
3. In the Search for field select Devices from the drop-down menu.
4. In the Search Criterias field, select Driver Name from the drop-down menu.
5. Select all Cisco drivers in use by NA.
6. Select Host Name from the Add Criteria drop-down menu.
7. Select does contain from the drop-down menu and enter: `redmond`
8. Select Configuration Text from the Add Criteria drop-down menu.
9. Select does not contain from the drop-down menu and enter: `set timezone PST`.
10. In the Boolean Expression field, modify the default string to read: A or (B and C).
11. Click the Search button.

Chapter 12: Managing Events and Diagnostics

Use the following table to quickly locate information.

Topic	Refer to:
Consolidated View of Events (SingleView)	“Consolidated View of Events (SingleView)” on page 552
Diagnostics	“Diagnostics” on page 555
Adding & Customizing Diagnostics	“Adding & Editing Custom Diagnostics” on page 558

Consolidated View of Events (SingleView)

SingleView enables you to track events that indicate changes to either a single device or all of your devices on one page. You can select from a list of event types, including:

- Device Booted
- Device Configuration Change
- Device Diagnostic Changed
- Device Password Change
- Device Reloaded
- Device Software Change
- Module Added
- Module Changed
- Module Removed
- Reserved Device Configuration Changed
- User Message

For a complete list of NA Events, refer to "Event Descriptions" on page 520.

To view the SingleView page, on the menu bar under Reports, click SingleView. The SingleView page opens.

SingleView Page Fields

Field	Description/Action
View Search Results as CSV File link	You are prompted for the location to save the displayed results as a CSV file.
Displayed Change Event Types link	Scrolls down to the Displayed Change Event Types menu, where you can select events to display.
For the:	Displays the time frame for viewing events. Options include: • Past 1, 2, 4, 8, 12, 24, and 48 hours • Past 1 and 2 weeks • Past 1 month • All Events
Current Working Group	Select a device group from the drop-down menu.
Check Boxes	You can use the left-side check boxes to delete events from the NA database. Once you have selected the events, click the Actions drop-down menu and click Delete. This deletes the selected events from the NA database. The adjacent Select drop-down menu enables you to select or deselect all of the events.
Event Date	Displays the date/time of the event in the format MMM-dd-yy HH:mm:ss. (The format is configurable by the System Administrator.)
Host Name	Displays the host name or IP address of the device. Clicking the Host Name or IP Address opens the Device Details page, where you can view information about the device and its configuration history.
Summary	Displays the type of event. For a list of NA Events, refer to "Event Descriptions" on page 520. Clicking the event type link opens the Event Detail page. This page includes: • The date and time the event occurred. • The login name of the person or process that added the event. • The event type. • A brief description of the event. • A link to detailed information about the device.
Added By	Displays the login name of the person whose action caused the event to be created.
Actions	The Compare to Previous link appears for the following events: • Device Configuration Change — Opens the Compare Device Configurations page. Refer to "Comparing Device Configurations" on page 181 for information. • Device Diagnostic Changed — Opens the corresponding comparison page, depending on the type of diagnostic that was changed, for example Compare NA Device File System page or the Compare NA Module Status page. • Device Password Change — Opens the Compare Device Configurations page. Refer to "Comparing Device Configurations" on page 181 for information.

Field	Description/Action
Displayed Change Event Types	Displays a list of event types from which you can select, including: • Device Booted • Device Configuration Change • Device Diagnostic Changed • Device Password Change • Device Reloaded • Device Software Change • Module Added • Module Changed • Module Removed • Reserved Device Configuration Changed • User Message

Diagnostics

In addition to configuration files, NA gathers other device information, such as routing tables, port statistics, and IP settings. Collectively, these are called *Diagnostics*. Diagnostics can help you determine the effects of configuration changes and troubleshoot complex issues such as routing problems and performance degradations.

By default, NA captures a basic set of diagnostics from a device each time NA detects a configuration change on that device. You can define additional diagnostic tasks or event rules to capture diagnostics at different times, and can define additional custom diagnostics to capture specific device information that is useful in your environment.

NA enables you to automatically launch diagnostics as a result of specific events. In addition, environmental diagnostics, such as CPU utilization, can be created and monitored so that automated reactions and responses can take place when certain thresholds are reached. Refer to "Adding Event Rules" on page 461 for information on automatically running a diagnostic as a result of a configuration change or other event.

On the menu bar under Devices, select Device Tools and click Diagnostics. The Diagnostics page opens. The available diagnostics are listed.

Diagnostics Page Fields

Field	Description/Action
New Diagnostic link	Opens the New Diagnostics page, where you can create a new diagnostic. Refer to "New Diagnostic Page Fields" on page 557 for information.
Run Diagnostics link	Opens the Run Diagnostics Task page, where you can run any diagnostic. Refer to "Run Diagnostics Task Page Fields" on page 312 for information.
Import/Export Diagnostics link	Opens the Import/Export Command Scripts/Diagnostics page, where you can import a pre-configured command script or diagnostic script, or export a command script or diagnostic script to a file. Refer to "Import/Export Scripts/Diagnostics Page Fields" on page 581 for information.
Check Boxes	You can use the left-side check boxes to delete diagnostics. Once you have selected the diagnostics click the Actions drop-down menu and click Delete. This deletes the selected diagnostics. The adjacent Select drop-down menu enables you to select or deselect all of the diagnostics.
Script Name	Displays the name of the diagnostic.
Mode/Device Family	Displays the device access mode in which the diagnostic runs, such as Cisco IOS enable.
Last Modified	Displays the date and time the diagnostic was last modified.
Partition	Diagnostics can be applicable to a specific Partition. All users can view diagnostics that are labeled [Shared] because they are applicable to all Partitions. **Note**: If the NA Administrator has partitioned devices, you can only view, edit, and run diagnostics that belong to a specific Partition (and the devices belonging to that Partition) for which you have permission to view. Refer to "Segmenting Devices and Users" on page 150 for information on segmenting devices and users.

Field	Description/Action
Last Modified by	Displays the name of the last user to modify the diagnostic (when available).
Actions	You can select from the following options: • Edit — Opens the Edit Diagnostic page, where you can edit the diagnostic. Refer to “New Diagnostic Page Fields” on page 557 for information. • Run — Opens the New Task - Run Diagnostics page, where you can run the diagnostic. Refer to “Run Diagnostics Task Page Fields” on page 312 for information.

New Diagnostic Page Fields

To create a new diagnostic:

1. On the menu bar under Devices, select Device Tools and click Diagnostics. The Diagnostics page opens.
2. Click the New Diagnostic link at the top of the page. The New Diagnostic Page opens. Be sure to click the Save Script button when you are finished.

Field	Description/Action
Diagnostics link	Opens the Diagnostics page, where you can create or run pre-defined diagnostics. Refer to "Diagnostics Page Fields" on page 555 for information.
Name	Enter the name of the diagnostic.
Description	Enter descriptive comments for the diagnostic.
Partition	Diagnostics can be applicable to a specific Partition. All users can view diagnostics that are labeled [Shared] because they are applicable to all Partitions. **Note**: If the NA Administrator has partitioned devices, you can only view, edit, and run diagnostics that belong to a specific Partition (and the devices belonging to that Partition) for which you have permission to view. Refer to "Segmenting Devices and Users" on page 150 for information on segmenting devices and users.
Advanced Scripting checkbox	If checked, Diagnostics can be defined as an advanced script without user-defined variables. The following fields replace the Mode and Driver fields: • Device Family — Select the name of the device family on which this script runs. A device family is a collection of devices that share a similar configuration CLI command syntax. • Language — Select the language in which the script was written. • Parameters — Enter the parameters for the script. Refer to "Adding Command Scripts" on page 582 for detailed information on creating advanced scripts.
Mode	Select the device access mode, such as Cisco Exec or Nortel Manager.
Driver	Select one of the following options: • All applicable drivers (the default) • Select specific drivers If selecting one or more drivers from the list, you can click one driver or use Shift+click or Ctrl+click to select multiple drivers. (**Note**: Devices that are menu-driven, such as the Baystack 470, cannot be accessed by custom diagnostics.)

Field	Description/Action
Script	Enter the device-specific commands to run. Keep in mind the height and width of the Script box is controlled by settings from the Administrative Settings option. If you use the scripting feature extensively, you may want to adjust these settings so that you can see the script without scrolling. **Note**: Scripts can exist with the same name, but different modes. This is how NA manages multi-vendor scripts. To run a script, simply select the script name. Each version of the script will load. When you run a script against a device group, NA knows the device type and applies the appropriate script.

To view diagnostics for a specific device:

1. On the menu tab under Devices, click Inventory.
2. Click the Host Name or IP Address of the device for which you want diagnostic information.
3. From the View drop-down menu, select Diagnostics and click the diagnostic you want to view. Each option shows a historical list of diagnostics specific to the device.

Adding & Editing Custom Diagnostics

NA enables you to define custom diagnostics to capture specific information that is useful in your environment. Because each user can run custom diagnostics, any user can analyze network problems, even though they may not have permission to modify the device configuration.

To define a custom diagnostic, you provide one or more commands to run on the device. NA stores the results of these commands as the diagnostic results. All users have permissions to run diagnostics, therefore it is important that these commands not change the device configuration. Custom diagnostics should perform read-only tasks.

You can use event rules to trigger diagnostics. For example, you could set a rule to run diagnostics whenever a configuration fails to deploy.

For multi-vendor networks, you can create multiple diagnostics with the same name, but running on different types of devices. Diagnostics with the same name are linked. When you run a group task, NA automatically runs the correct version of the diagnostic for each device. For example, you could run a group diagnostic to collect data on all your routers in San Francisco, even if the routers are from multiple vendors.

Note: You must periodically purge old data from the NA database. While it is important to purge all your old data periodically to maintain performance and restore disk space, it is especially important to purge diagnostic and script data. Unlike configurations, which are stored only when they differ from their previous instance, all diagnostic and script data is stored. By default, NA purges diagnostic data after 45 days. Refer to "Data Pruning Task Page Fields" on page 387 for information.

Chapter 13: Custom Data Setup

Use the following table to quickly locate information.

Topic	Refer to:
Getting Started	"Getting Started" on page 560
Custom Data Setup Page Fields	"Custom Data Setup Page Fields" on page 560
Enhanced Custom Fields Setup	"Enhanced Custom Fields Setup" on page 564

Getting Started

The purpose of custom data fields is to enable you to assign useful data to specific devices, configurations, users, and so on. This gives you added flexibility and enables you to integrate NA with other applications.

By default, HP Network Automation (NA) supports up to six custom data fields. Enhanced custom data fields provide up to 25 additional custom data fields for the Device Details and Device Interfaces pages. For information about enabling enhanced custom data fields, see "Enhanced Custom Fields" on page 64. For information about configuring enhanced custom data fields, see "Enhanced Custom Fields Setup" on page 564. For information about enabling more than 25 enhanced custom fields, see the *NA Administration Guide*.

Previously, several CLI commands had the ability to modify a custom field through the use of the `customname` and `customvalue` options on the command. However, you could only manipulate one field at a time. This was cumbersome if you needed to modify multiple fields. As a result, the new `customnames` and `customvalues` values enable you to specify multiple fields to modify simultaneously.

Note that the names and values are in comma separated lists. If you have a value that includes a comma, be sure to put it in single quotes. For example:

```
mod device -customnames "Location, Floor, Rack" -customvalues "'Seattle,
WA',3rd,'126-18,10'"
```

Note: The old options are still available to preserve backward compatibility of existing scripts.

To add custom data, on the menu bar under Admin click Custom Data Setup. The Custom Data Setup page opens.

Custom Data Setup Page Fields

Field	Description/Action
Custom Data Setup	Select a custom data setup from the drop-down menu. Options include: • Device Configurations & Diagnostics • Devices • Device Blades/Modules • Device Interfaces • Device Groups • Users • Tasks • Telnet/SSH Sessions
Check Boxes	You can use the left-side check boxes to enable the field. Consequently, the field appears in the user interface and is available to the integration API.

Field	Description/Action
Device Configuration & Diagnostics	
These fields appear on the Device Configuration Detail page. You can enter or edit the values by clicking the Edit Comments link, which opens the Edit Device Configuration Detail page.	
API Name	Identifies the field to the integration API and notification rules. You can use A-Z, a-z, 0-9, _, -, & (not including the comma) in an API name.
Display Name	Displays the name that users see in the user interface.
Values	Select one of the following options: • Can contain HTML — If checked (the default) users (or the integration API) are expected to enter HTML code in this field. NA displays the field as HTML, not text, in the user interface. This enables you to include a link to an external trouble ticket application. • Limit to — If checked, enter values, separated by commas, that will appear in a drop-down list box.
Devices	
These fields appear on the Device Information page. You can enter or edit the values by clicking the Edit link, which opens the Edit Device page, or by clicking Add from the Devices drop-down menu, which opens the New Device page.	
API Name	Identifies the field to the integration API and notification rules. You can use A-Z, a-z, 0-9, _, -, & (not including the comma) in an API name.
Display Name	Displays the name that users see in the user interface.
Values	Select one of the following options: • Can contain HTML — If checked (the default) users (or the integration API) are expected to enter HTML code in this field. NA displays the field as HTML, not text, in the user interface. This enables you to include a link to an external trouble ticket application. • Limit to — If checked, enter values, separated by commas, that will appear in a drop-down list box.
Device Blades/Modules	
These fields appear on the View/Edit Modules pages.	
API Name	Identifies the field to the integration API and notification rules. You can use A-Z, a-z, 0-9, _, -, & (not including the comma) in an API name.
Display Name	Displays the name that users see in the user interface.
Values	Select one of the following options: • Can contain HTML — If checked (the default) users (or the integration API) are expected to enter HTML code in this field. NA displays the field as HTML, not text, in the user interface. This enables you to include a link to an external trouble ticket application. • Limit to — If checked, enter values, separated by commas, that will appear in a drop-down list box.

Field	Description/Action
Device Interfaces	
These fields appear on the View/Edit Modules pages.	
API Name	Identifies the field to the integration API and notification rules. You can use A-Z, a-z, 0-9, _, -, & (not including the comma) in an API name.
Display Name	Displays the name that users see in the user interface.
Values	Select one of the following options: • Can contain HTML — If checked (the default) users (or the integration API) are expected to enter HTML code in this field. NA displays the field as HTML, not text, in the user interface. This enables you to include a link to an external trouble ticket application. • Limit to — If checked, enter values, separated by commas, that will appear in a drop-down list box.
Device Groups	
These fields appear on the Device List page for the group. You can enter or edit the values by clicking the Edit Group link, which opens the Edit Group page, or by clicking Groups from the Devices drop-down menu, which opens the New Group page.	
API Name	Identifies the field to the integration API and notification rules. You can use A-Z, a-z, 0-9, _, -, & (not including the comma) in an API name.
Display Name	Displays the name that users see in the user interface.
Values	Select one of the following options: • Can contain HTML — If checked (the default) users (or the integration API) are expected to enter HTML code in this field. NA displays the field as HTML, not text, in the user interface. This enables you to include a link to an external trouble ticket application. • Limit to — If checked, enter values, separated by commas, that will appear in a drop-down list box.
Users	
These fields appear on the My Profile page. You can enter or edit the values by clicking the Edit link on the User List page, which opens the Edit User page, or by clicking New User on the User List page, which opens the New User page.	
API Name	Identifies the field to the integration API and notification rules. You can use A-Z, a-z, 0-9, _, -, & (not including the comma) in an API name.
Display Name	Displays the name that users see in the user interface.
Values	Select one of the following options: • Can contain HTML — If checked (the default) users (or the integration API) are expected to enter HTML code in this field. NA displays the field as HTML, not text, in the user interface. This enables you to include a link to an external trouble ticket application. • Limit to — If checked, enter values, separated by commas, that will appear in a drop-down list box.

Field	Description/Action
Tasks	
These fields appear on Task pages. You cannot enter or edit the values through the user interface, but only through the integration API.	
API Name	Identifies the field to the integration API and notification rules. You can use A-Z, a-z, 0-9, _, -, & (not including the comma) in an API name.
Display Name	Displays the name that users see in the user interface.
Values	Select one of the following options: • Can contain HTML — If checked (the default) users (or the integration API) are expected to enter HTML code in this field. NA displays the field as HTML, not text, in the user interface. This enables you to include a link to an external trouble ticket application. • Limit to — If checked, enter values, separated by commas, that will appear in a drop-down list box.
Telnet/SSH Sessions	
These fields appear on the Telnet/SSH Session List page. You cannot enter or edit the values through the user interface, but only through the integration API.	
API Name	Identifies the field to the integration API and notification rules. You can use A-Z, a-z, 0-9, _, -, & (not including the comma) in an API name.
Display Name	Displays the name that users see in the user interface.
Values	Select one of the following options: • Can contain HTML — If checked (the default) users (or the integration API) are expected to enter HTML code in this field. NA displays the field as HTML, not text, in the user interface. This enables you to include a link to an external trouble ticket application. • Limit to — If checked, enter values, separated by commas, that will appear in a drop-down list box.

Enhanced Custom Fields Setup

Custom fields enable you to assign useful data to specific devices. This gives you added flexibility and enables you to integrate NA with other applications.

Note: Before you can add enhanced custom fields, you must enable the Enhanced Custom Fields application. Refer to "User Interface Page Fields" on page 63 for instructions.

To view the current custom fields and add data to the Device Details and Device Interfaces pages, on the menu bar under Admin click Extended Custom Fields Data Setup. The Enhanced Custom Fields Data Setup page opens.

Field	Description/Action
Drop-down menu	Select one of the following options from the drop-down menu: • Devices (the default) • Device Interfaces
Add Custom Devices Field link	Clicking the Add Custom Devices Fields link opens the New Custom Data Field page, where you can add custom data fields. These data fields are displayed on the Device Details and Device Interfaces pages. Refer to "New Custom Data Field Page" on page 565 for information. For information on the Device Details and Device Interfaces pages, refer to "View Menu Options" on page 203 and "Device Interfaces Page Fields" on page 207.
Devices / Device Interfaces	
Enabled	Indicates if the custom data field is enabled.
Field Name	Displays the name of the custom data field.
Limit Values To	Displays a list of comma separated values. The list is shown as a drop-down menu when editing the actual data.
Allow HTML	Indicates if users can enter HTML code in this data field. NA displays the data field as HTML, not text.
Actions	Select one of the following options: • Edit — Opens the Edit Custom Data Field page, where you can edit the current information. Refer to "New Custom Data Field Page" on page 565. • Delete — Enables you to delete Custom Data Fields. Deleting a data field will cause any data associated with that field to be deleted as well.

New Custom Data Field Page

To add custom data to the Device Details and Device Interfaces page, on the menu bar under Admin click Enhanced Custom Fields Setup. The enhanced Custom Fields Setup page opens. Click the Add Custom Devices Field link at the top of the page.

Field	Description/Action
Enabled	If checked, the custom data field is enabled.
Field Name	Enter a data field name.
Limit Values To	Enter a list of comma separated values. The list is shown as a drop-down menu when editing the actual data.
Allow HTML	If checked, users can enter HTML code in this field. NA displays the field as HTML, not text.

Click the Save button when you are done. The new field is displayed on the Enhanced Custom Fields Setup page.

Chapter 14: Creating Configuration Templates

Use the following table to quickly locate information.

Topic	Refer to:
Getting Started	"Getting Started" on page 568
Viewing Configuration Templates	"Viewing Configuration Templates" on page 569
Creating New Configuration Templates	"Creating New Configuration Templates" on page 571

Getting Started

Configuration templates enable rapid, straightforward deployment of new device configurations. Using configuration templates:

- Engineers can provision devices or services quickly while conforming to departmental configuration standards.
- Network architects can create friendly GUI prompts with validation parameters so that template users can fill in the blanks to rapidly populate and deploy new configurations.

In general, configuration templates are fragments of configuration data that can be assembled in various ways to form a script. In turn, this script can add to data already on a device or replace parts of a configuration.

For information on creating device templates, refer to "Device Templates" on page 120.

After you create a configuration template and populate it with commands, you can create a script from the template. When you run the script, it deploys the configuration commands, either as a fragment or an entire configuration, to one or more devices.

Viewing Configuration Templates

To view the current configuration templates, on the menu bar under Devices, select Device Tools and click Configuration Templates. The Configuration Templates page opens. Use this page to view a list of configuration templates sorted by vendor.

Configuration Templates Page Fields

Field	Description/Action
New Configuration Template link	Opens the New Configuration Template page, where you create a new configuration template. Refer to "Creating New Configuration Templates" on page 571 for information.
Vendor	Displays the vendor for the devices to which this configuration template applies. Clicking the Vendor link opens the Configuration Templates page, where you can view the templates for this vendor. From this page, you can: • Include the configuration template in a script and build a full script from them. • Create a new configuration template.
Check Boxes	You can use the left-side check boxes to delete configuration templates. Once you have selected the templates, click the Actions drop-down menu and click Delete. This deletes the selected configuration templates. The adjacent Select drop-down menu enables you to select or deselect all of the configuration templates.
Name	Displays the name of the configuration template.
Partition	If you have created Partitions for security or business reasons, you can partition configuration templates for each device in a specific Partition. Keep in mind that you can configure templates to be shared by all devices in all Partitions, as well as for specific devices in specific Partitions. Refer to "Segmenting Devices and Users" on page 150 detailed information on creating Partitions. **Note**: This field is only displayed if you have configured one or more Partitions. In general, a Partition is a grouping of devices with unique IP addresses. Multiple Partitions can be managed by a single NA Core. A NA Core in an installation of a NA server, comprised of a single Management Engine, associated services, and a single database.
Role	Displays the role of the configuration template. The default roles include: • Any • Core • Border • Test
Model	Displays the model of the devices to which this configuration template applies.
Processor/ Component	Displays the processor of the devices to which this configuration template applies.
Drivers	Displays the drivers assigned to the devices to which this configuration template applies.

Field	Description/Action
Actions	You can select one of the following options: • View Details — Opens the View Configuration Template page, where you can view the configuration template as HTML in a separate browser window. Refer to "View Configuration Template Page Fields" on page 573 for information. • View Text — Opens a text window, where you can view the configuration template as text in a separate browser window. Refer to "View Configuration Template Page Fields" on page 573 for information. • Edit — Opens the Edit Configuration Template page, where you can add or edit a configuration template. Refer to "New Configuration Template Page Fields" on page 571 for information.

Creating New Configuration Templates

To create a new configuration template:

1. On the menu bar under Devices, select Device Tools and click Configuration Templates. The Configuration Templates page opens.
2. Click the New Template link at the top of the page. The New Configuration Template page opens. Be sure to click the Save Template button when finished.

New Configuration Template Page Fields

Field	Description/Action
Templates link	Opens the Configuration Templates page, where you can view all of the current configuration templates. Refer to "Viewing Configuration Templates" on page 569 for information.
Name	Enter the name of the configuration template.
Partition	Select a Partition from the drop-down menu. (**Note**: This field is only displayed if you have configured one or more Partitions.) If you have created Partitions for security or business reasons, you can partition configuration templates for each device in a specific Partition. Keep in mind that you can configure templates to be shared by all devices in all Partitions, as well as for specific devices in specific Partitions. Refer to "Segmenting Devices and Users" on page 150 for detailed information on creating Partitions.
Comments	Enter a description of the configuration template. Comments are included in all tables, so include only crucial information.
Role	Select a role for the configuration template. Default roles include: • Any • Core • Border • Test
Model	Enter the model of the devices to which this applies.
Processor/ Component	Enter the processor of the devices to which this configuration template applies.
Mode	Select the device command line interface (CLI) mode in which the configuration template runs. (**Note**: Commands should not change the CLI prompt or mode. Otherwise, the script will stop running at that command and return an error.)
Driver	Select one of the following options: • All applicable drivers (the default) • Select specific drivers — Select the driver assigned to the devices to which this configuration template applies. The list includes only drivers that are compatible with the selected mode.

Field	Description/Action
Template	Enter the configuration commands and comments that populate the configuration template. Each line you enter should represent one complete command for the device. After the command, you should see the device's prompt again. When the configuration template is applied to devices, this configuration will be deployed. Keep in mind that variable names cannot begin with tc_, but can include any combination of uppercase alpha, lowercase alpha, 0 through 9, and underscore characters.

View Configuration Template Page Fields

To view a specific configuration template:

1. On the menu bar under Devices, select Device Tools and click Configuration Templates. The Configuration Templates page opens.
2. Click the View Details option in the Actions column for the configuration template you want to view. The View Configuration Template page for that template opens.

Field	Description/Action
Edit Template link	Opens the Edit Configuration Template page, where you can create a new configuration template. Refer to "New Configuration Template Page Fields" on page 571 for information.

Text Version link	Opens a text window, where you can view the configuration template as text in a separate browser window. The text would look something like the following:
	`sflow destination $dest_ip_1$ $dest_udp_port1$`
	`sflow destination $dest_ip_2$ $dest_udp_port2$`

Template link	Opens the Configuration Templates page, where you can view a list of configuration templates sorted by vendor. Refer to "Configuration Templates Page Fields" on page 569 for information.
Comments	Displays comments entered by the configuration template author or edited later. (**Note**: The Comments box is hidden unless populated.)
Line	Displays the number of each line in the configuration template.
Template Text	Displays the configuration commands and comments that populate the configuration template.
Name	Displays the name of the configuration template.
Partition	If you have created Partitions for security or business reasons, you can partition configuration s for each device in a specific Partition. Keep in mind that you can configure templates to be shared by all devices in all Partitions, as well as for specific devices in specific Partitions. Refer to "Segmenting Devices and Users" on page 150 for detailed information on creating Partitions.
Model	Displays the model of the devices to which this configuration template applies.
Last Modified By	Displays the user or process that last modified the configuration template.
Role	Displays the role of the configuration template. The default roles include: • Any • Core • Border • Test
Last Modified Date	Displays the date the configuration template was last modified.
Processor/ Component	Displays the processor of the devices to which this configuration template applies.

Field	Description/Action
Mode	Displays device command line interface (CLI) mode in which the configuration template runs.
Drivers	Displays the drivers assigned to the devices to which this configuration template applies.

Chapter 15: Managing Command Scripts

Use the following table to quickly locate information.

Topic	Refer to:
Getting Started	"Getting Started" on page 576
Adding & Editing Command Scripts	"Adding Command Scripts" on page 582
Running Command Scripts	"Running Command Scripts" on page 596
Creating Auto-remediation Scripts	"Creating Auto-remediation Scripts" on page 587
Importing and Exporting Command Scripts and Diagnostics	"Import/Export Scripts/Diagnostics Page Fields" on page 581

Getting Started

You can define command scripts to run a set of commands on one or multiple active devices. Command scripts are particularly useful for batch actions on a group of devices. For example, you could run a script on the Inventory group to update all devices to match standard policies, such as setting the SNMP trap logging host, NTP server, or a corporate login banner.

The Advanced Scripting feature enables you to run custom scripts written in various command line languages, such as Expect and PERL. Advanced scripting enables the extended capability of conditional logic. Because advanced scripts must support a fully functional Expect engine, external Telnet/SSH clients are called and run in a separate process. Refer to “New Command Script Page Fields” on page 584 for more information on the Advanced Scripting feature.

Note: Language support must be installed to use the Advanced Scripting feature. In addition, you must configure the Administrative Settings to enable it. Support for the Expect language is installed with NA. Windows environments with PERL scripting capability must install PERL (CPAN).

HP Operations Orchestration (HP OO) Flows

To run HP Operations Orchestration (HP OO) flows via an advanced command script:

1. Make sure HP Operations Orchestrations Authentication setup is configured correctly. Refer to “User Authentication” on page 75 for information.
2. Check the Advanced Scripting box and select “Flow” as the language. Advanced scripting instructs NA to use the “Flow” language type. Otherwise NA would try to interpret the syntax as device syntax, such as IOS.
3. In the Script field, enter: `/PAS/services/http/execute/Library/<path to flow>?flowvariable=value,flowvariable2=value2`

Note: You can still use command script variables as needed, and any number of HP OO flow input variables. Refer to the *HP Operations Orchestration Software Development Kit Guide* for information on using HP OO.

Bare Metal Provisioning Scripts

Bare metal provisioning scripts enable you to bring a bare metal device to a state that can be accessed by a NA device driver. Creating a bare metal script is the same as creating a standard command script. All custom script variables are available in the bare metal script. However, when creating bare metal scripts, you must:

- Select Bare Metal Script as script type
- Select one of the Bare Metal modes
- Name the command script appropriately, including the device family on which the script is designed to run

Note: Although you can use advanced scripting when you select the Bare Metal Script type, it is recommended that you do not select the “advanced script” checkbox.

Refer to “Edit Device Page Fields” on page 113 for detailed information on bare metal provisioning.

A typical bare metal script scenario would be as follows:

1. Rack mount the device.
2. Setup the console access to the device (or possibly a management IP address).
3. Login to NA.
4. On the menu bar under Devices, select New and click Device. The New Device page opens. Refer to “Adding Devices” on page 108 for detailed information on adding devices to NA.
5. Add the device to NA with following information:
   - IP Address
   - Host name
   - Passwords
   - Console address/port (if the device has not been configured with an accessible management IP address)
   - Other appropriate device fields
6. Select a Management Status of Pre-Production.
7. Specify a bare metal driver for this device.
8. Save the device. The Device Details page opens.
9. From the Provision menu, click Run Command Script. The Run Command Script page opens. The page is automatically populated with bare metal script lists. Refer to “Running Command Scripts” on page 596.
10. Select a bare metal script that is appropriate to the device and provide the values for the script variables if required.
11. Run the script. If the script succeeds, a Discovery task is automatically scheduled if you have enabled the “Run driver discovery task” option on the Run Command Script page. Note that you can disable this option if needed.

12. If the Discovery task succeeds, the device moves from the bare metal stage to a pre-production device.

Below is a sample bare metal script for a Cisco 2800 device.

```
#scriptvar.carriage_return="\r"
#scriptvar.command_delay="3"
#scriptvar.baremetal_timeout="5"
#scriptvar.success_pattern=/Building configuration/
yes
yes
$tc_device_hostname$
$tc_device_password$
$legacy_enable_password$
$tc_device_enable_password$
no
FastEthernet0/0
yes
no
yes
$tc_device_ip$
$network_mask$
2
```

Keep the following in mind when creating bare metal scripts:

- On top of the bare metal script, you can choose to define some script settings (all optional). These lines always start with `#scriptvar`.
- Carriage_returns define the format of the line break that is sent to the device for each command. This can be \r, \n, \r\n, or none (no linebreaks are sent after each command).
- Command_delays define the wait time (in seconds) before NA sends the next command to device in the script.
- Baremetal_timeout defines the Expect timeout for the command.
- Success_patterns define a regular expression pattern. When a valid success pattern is specified, the task will be considered successful only when such a pattern is matched with the device output.

Viewing Command Scripts

To view a list of pre-defined and custom command scripts, on the menu bar under Devices, select Device Tools and click Command Scripts. The Command Scripts page opens. The page displays a list of command scripts for which you have permissions. Users with full access to command scripts see a selection of pre-defined scripts delivered with NA.

Command Scripts Page Fields

Field	Description/Action
New Command Script link	Opens the New Command Script page, where you can write a new script and pull variables from the script to define prompts. Refer to "New Command Script Page Fields" on page 584 for information.
Run Command Scripts link	Opens the Run Command Script Task page, where you can set up a task to run command scripts. Before saving the task, you can edit variables in the script to create a unique instance of the script. Refer to "Run Command Script Task Page Fields" on page 306 for information.
Import/Export Commands Scripts link	Opens the Import/Export Command Scripts/Diagnostics page, where you can import a pre-configured command script or export a command script to a file. Refer to "Import/Export Scripts/Diagnostics Page Fields" on page 581 for information.
Script Type	The Script Type drop-down menu enables you to filter the list of scripts to view only scripts of a specific type.
Check Boxes	You can use the left-side check boxes to delete scripts. Once you have selected the scripts, click the Actions drop-down menu and click Delete. This deletes the selected scripts. The adjacent Select drop-down menu enables you to select or deselect all of the scripts.
Script Name	Displays the name of the script.
Mode / Device Family	Displays the device access mode, such as Cisco Exec or Nortel Manager, in which the script runs. Device Family is used for Advanced Scripting and displays a collection of devices that share a similar configuration CLI command syntax.
Last Modified	Displays the date and time the script was last modified.
Partition	Command script and/or diagnostics can be applicable to a specific Partition. All users can view command scripts and/or diagnostics that are labeled "global" because they are applicable to all Partitions. **Note**: If the NA Administrator has partitioned devices, you can only view, edit, and run command scripts and/or diagnostics that belong to a specific partition for which you have permission to view. Refer to "Segmenting Devices and Users" on page 150 for information on segmenting devices and users.
Last Modified By	Displays the name of the last user to modify the script. For example, if the script is a script template, this field shows who modified the script for a specific instance.

Field	Description/Action
Actions	You can select one of the following options: • Edit — Opens the Edit Command Script page, where you can modify an existing script. Refer to “New Command Script Page Fields” on page 584 for information. • Run — Opens the Run Command Script Task page, where you can run the command script. Refer to “Run Command Script Task Page Fields” on page 306 for information.

Import/Export Scripts/Diagnostics Page Fields

When you click the Import/Export Commands Scripts link on the Command Scripts page, the Import/Export Scripts/Diagnostics page opens.

Field	Description/Action
Import	Select the content to import. • To import a command script or diagnostic from a non-driver source, select **Import from file**, and the enter the file name or click **Browse**. • To import a command script or diagnostic from an NA-provided device driver, select **Import from driver**, and then select from the list of drivers that contain custom content. Click **Import**, select the scripts to import, and then click **Continue**. If the command script or diagnostic script already exists, you are prompted to rename it.
Export Scripts/ Diagnostics	Displays a list of the current command scripts and diagnostic scripts. Click the scripts you want to export and then click the Export button.

Adding Command Scripts

Command scripts enable you to:

- Run a custom set of commands on one or more devices.
- Run scripts as a scheduled task, and use event rules to trigger scripts to run. For example, you could set a rule to configure standard settings on a particular device type whenever a device of that type is added.

NA provides several options for adding scripts. You can:

- Write or copy a script into the New Command Script page, adding variables or defining prompts as needed.
- Create template scripts that enable users to edit variable values before running a script. "Creating a Script from a Configuration Template" on page 596 for information.
- Convert a session log to an Expect or Perl script. Because NA installs Expect, the Convert to Expect script link is automatically available. The Convert to Perl script link is only displayed if Perl is configured as a scripting language in the Administrative Settings. Refer to "Server Page Fields" on page 54 for information. Keep in mind that the Convert to Perl script link requires the *Opsware::NA::Connect Perl* module that is installed when NA is installed.

NA supports both simple and advanced scripting.

Simple scripting is mode-based (CLI command language). Keep in mind that simple command scripts do not recognize device CLI errors. Consequently, NA assumes the device CLI commands executed were successful. A simple command script only fails if it cannot reach the device or it loses connection to the device during the execution of the script.

Advanced scripting is based on any command line scripting language, such as Expect or PERL, including scripts that contain conditional logic (*if*, *while*, and *for* conditions). You can customize instances of a script by including variables. When you run the script, you are prompted for a value for each variable. Refer to the following table for additional details.

Note: Character '$' is reserved for the variable name. Use escape sequence \x24 if you need to enter a literal '$' in a script.

Simple Scripts	Advanced Scripts
• No if or loops • Uses device command (Cisco commands like *show conf)* • No error handling • No login required • No NA device variables	• If and loops permitted • Uses language commands (PERL or Expect commands such as send "show conf\n" or print SOCKET "show conf\n") • Can handle errors • Requires code to login • Can access NA device variables

You can use scripts to perform the same task on different types of devices by creating multiple scripts with the same name so that all scripts by that name run as a single task. (The devices must be configured as a device group.) When you run the script, you see every instance of the script that applies to any device in the group. For example, you could run a script to change the NTP server on all your routers, even if the routers are from different vendors. When running multiple scripts of the same name, you can edit each instance of the script.

To add a new command script:

1. On the menu bar under Devices, select Device Tools and click Command Scripts. The Command Scripts page opens.
2. Click the New Command Script link at the top of the page. The New Command Script page opens. Be sure to click Save Script when you are finished. When the script is saved successfully, the Command Scripts page opens. The script you added appears in the list and is highlighted. Keep in mind that a script does not run until you schedule it as a task.

Note: Variables beginning with “tc_” are reserved for special use. You cannot define any variables in custom or advanced scripts that begin with this character sequence.

New Command Script Page Fields

Command scripts enable you to:

- Run a custom set of commands on one or more devices.
- Run scripts as a scheduled task, and to use event rules to trigger scripts to run. For example, you could set a rule to configure standard settings on a particular device type whenever a device of that type is added.

When you create a command script, you can define your own custom variables, such as *$MyVar$*. Custom variables are displayed as user-supplied variables on the Run Command Script Task page.

If you would rather have custom variables supplied in a CSV file, you can replace the existing scriptField1, scriptField2, and so on headers with the custom variables from your script. As a result, when you go to run the command script, any custom variables in the script (also referenced in the CSV file) are noted in the Run Command Script Task page’s Task Options/Variables field as Provided in the CSV data file.

Any custom variables defined in the script, but not referenced in the CSV file, are displayed for user input. Refer to “Run Command Script Task Page Fields” on page 306 for information.

Field	Description/Action
Command Scripts link	Opens the Command Scripts page, where you can view the list of command scripts. Refer to “Command Scripts Page Fields” on page 579 for information.
Name	Enter the name of the new script.
Description	Enter a description of the script, for example whether it was created from a template and who created it.
Partition	Scripts and/or diagnostics can be applicable to a specific Partition or globally. All users can view scripts and/or diagnostics that are labeled “global” because they are applicable to all Partitions. You can select a specific Partition from the drop-down menu. **Note**: If the NA Administrator has partitioned devices, you can only view, edit, and run scripts and/or diagnostics that belong to a specific partition for which you have permission to view. Refer to “Segmenting Devices and Users” on page 150 for information on segmenting devices and users.
Script Type	Select one of the following options: • General Purpose (the default) • Existing — Select a script from the drop-down menu. • New — Enter a new script type.

Field	Description/Action
Advanced Scripting	If checked, the page is refreshed to provide settings specific to custom scripts written in command line languages such as Expert and PERL. Advanced Scripting specific fields include: • Device Family — A device family is a collection of devices that share a similar configuration CLI command syntax. Select a device family. This restricts the script to run against those devices whose driver is in the selected device family. This feature enables you to assign one name to multiple implementations of a script created for different devices so that they can run as a single task. • Language — Select the scripting language in which the script you are adding is written. You must install language support and configure the language in Administrative Settings/Server/Advanced Scripting to use this feature. Options include Expect, Perl, and Flow. (**Note**: Expect support is installed with NA, but you must still configure the path.) For information on Flow, refer to "HP Operations Orchestration (HP OO)" on page 78. • Parameters — Enter the authentication parameters for the script. You can include NA or your own custom variables. (**Note**: Using parameters for authentication is recommended as this strategy reduces the security risk of having passwords written to a file.) • Script — Advanced Scripting commands can contain conditional logic and include pre-defined variables. Variable names can only contain letters, numerals and underscores (_). The required format is the variable name between two dollar signs ($), as illustrated in these examples: $report$, $my_address$, $port_3_ip$. Advanced scripts must include any code required to connect and log in to the device. For example, you can connect to tc_device_ip and log in using $tc_device_password$. • Device variables link — Displays a list of device variables available for use in your advanced custom scripts. These variables always begin with $tc_ and the names are case sensitive. (You can also create your own variables.) • Pull Variables button — Refreshes the page, adding input fields at the bottom of the page for each variable used in the script. Use these fields to define custom prompts for the variables and to limit the values that each prompt will accept. You can select the following options for each variable: - allow multiple lines in value - Limit Values To: (first,last,next-to-last) - Password (If checked, NA does not echo the password when prompting for a value on the Run Command Script Task page.
Mode	Select the device access mode, such as Cisco Exec or Nortel Manager.
Driver	Select one of the following options: • All applicable drivers (the default) • Select specific drivers — If selecting one or more drivers from the list, you can click one driver or use Shift+click or Ctrl+click to select multiple drivers. (**Note**: Devices that are menu driven, such as the Baystack 470, cannot be accessed by custom scripts.)
Script	Enter the device-specific commands to send to the device, or paste in and edit an existing script. Refer to the help information on the Command Script page regarding how commands must be entered. **Note**: Variable names cannot begin with tc_ (reserved for NA), but can include any combination of uppercase alpha, lowercase alpha, 0 through 9, and underscore characters.

Field	Description/Action
Pull Variables button	Refreshes the page, adding input fields at the bottom of the page for each variable used in the script. Use these fields to define custom prompts for the variables and to limit the values that each prompt will accept. Sample fields include: • HOSTNAME • ETH_SLOT1 Enter the custom prompt you want the user to respond to when this script runs, and the response values you want this prompt to accept. Values must be separated by commas, so you cannot use values that include commas. If you specify multiple values, when the user sees the prompt, a list of accepted values is provided in the prompt dialog.

Creating Auto-remediation Scripts

An Auto-remediation script enables you to define variables in the script that reference data from regular expression pattern groups in a violated policy rule. Auto-remediation variables can also be used with non-regular expression patterns.

Auto-remediation scripts are different from standard command scripts. Given the possibility of complex policy definitions, Auto-remediation scripts must have basic language constructs, such as `for-loop` and `if-statements`, requiring a pre-processing step to generate the actual command script to run on a device.

Auto-remediation scripts include syntax to enable you to iterate over matches. The Auto-remediation script is converted to a command script with regular expression variable substitutions. The template processor (command script generator) parses and generates an executable command script, which is then run by the Auto-remediation task.

To add a new Auto-remediation script, refer to "New Rule Page Fields" on page 422.

Auto-remediation Script Syntax

NA includes new Auto-remediation script syntax to be able to access violation data. The following table describes the scripting language elements used in Auto-remediation scripts.

Language Element	Description
`@foreach`	Loop syntax to iterate over matched lines.
`@ifexists`	Control syntax to test whether a variable has a match.
`@end`	Indicates the end of `@foreach` or `@ifexists`.
`$loop_variable$`	Any variable name that you want to use to iterate over matches of a regular expression pattern line in a condition.
`$line_match_variable$`	Represents an array of configuration lines that are matched for a regular expression pattern line of a condition. For example, configuration lines matched for first line of Condition A: `$condition_A_line_1$`.
`$regex_group_match_ variable$`	Represents the text that is matched for a regex group.
`@`	The prefix for Auto-remediation language elements so as to distinguish them from device commands.
`//`	The prefix to comment out a line in an Auto-remediation script.

Auto-remediation Script Variable Naming Conventions

The following table describes the Auto-remediation script naming conventions.

Variable	Naming Convention	Example
Loop	`$any_string$`	`$interface$`— Each config line that matches a regex pattern.
Pattern line match (that represents matches for a line of a regex pattern)	`$condition_<label>_line_<number>$`	`$condition_A_line_2` — Config lines that match for the second line of Condition A.
Regex group match	`$<loop_variable>.regex_group_<number>$`	`$interface.regex_group_1$`— Match for the first regex group in a config line that matched the regex pattern. • number = 0: whole match • number > 0: regex capturing groups
Block start pattern	`$block_start$`	Built-in variable name for the block start pattern.
Block end pattern	`$block_end$`	Built-in variable name for the block end pattern.

Notes:

- `@foreach $loop_variable$` in `$line_match_variable$`, where `$loop_variable$` is used to represent each matched line of `$line_match_variable$`: the array of matches for a line of a regex pattern in a condition. For example, `$condition_A_line_1$` is a match variable that represents all configuration lines that are matched for the first line of Condition A.
- `@ifexists $regex_group_match_variable$`, where the `$regex_group_match_variable$` is used to represent matches for a regular expression group.
- Nested `@foreach` loops are allowed.
- Block start and end patterns are accessed by `$block_start$` and `$block_end$` array variables. (Refer to Example 3 on page 639.)
- Regular expression groups are part of the regular expression patterns that are enclosed in parentheses. For example, pattern `interface (.*)`, `(.*)` is a regular expression group (also called capturing group).
- Violation data is available for “must not contain” and “must contain only” operators. There is no violation data for the “must contain” operator because violations occur when there is no match for a pattern using the “must contain” operator. Keep in mind you can write an Auto-remediation script without any variable references. As a result, no Auto-remediation script syntax elements are used.
- Auto-remediation variables can be used with non-regular expression patterns. As a result, there will be no regular expression group variables; the entire match can be

accessed with a group zero variable (for example: `$matching_line.regex_group_0$` where `$matching_line$` is a `@foreach` loop variable).

- The Auto-remediation task runs as a Run Command Script task. However, what is actually run on the device is a command script that is generated by the Auto-remediation script pre-processing engine before the Run Command Script task is scheduled. Refer to "Run Command Script Task Page Fields" on page 306 for information on running command scripts.
- Auto-remediation scripts must be enabled from the "Configuration Policy Verification" section on the Configuration Management page. Refer to "Configuration Management" on page 37 for information.

Auto-remediation Script Examples

Example 1: No Violation Data (simplest case)

The simplest Auto-remediation scripts are used with the "must contain" operator because the results do not produce violation data. As a result, the script does not require any Auto-remediation script syntax.

Assume the following condition (note that the patterns are not regular expressions):

```
Condition A: Config Text
must contain
  ntp server 169.243.103.34
  ntp server 170.242.62.16
  ntp server 170.242.62.17
  ntp server 169.243.226.94
```

When the configuration text does not include the lines in the pattern, Condition A is violated. To fix the violation, the following Auto-remediation script inserts the lines into the configuration:

```
Script:
   ntp server 169.243.103.34
   ntp server 170.242.62.16
   ntp server 170.242.62.17
   ntp server 169.243.226.94
```

As noted above, there is no need to use Auto-remediation script syntax in the script.

Example 2: Violation Data

The following example illustrates how to use Auto-remediation with violation data references. Note that this is only an example and is not to be used in a real case.

Assume we want to check the following lines in a configuration against the condition given below (which includes two regular expression pattern lines):

```
Configuration text:
       ...
       access-list 139 deny   ip host 192.168.139.1 any
       access-list 139 deny   ip host 192.168.139.2 any
       access-list 139 permit ip any any
       ...


Condition A: Config Text
must not contain
  access-list (.*) deny   ip host (.*) any
  access-list (.*) permit (192\.0\.0\..*)
```

The following lines in the above configuration text will violate the condition:

```
access-list 139 deny ip host 192.168.139.1 any
access-list 139 deny ip host 192.168.139.2 any
```

The two lines will be placed in the `$condition_A_line_1$` array variable because they are matched against the first pattern line of Condition A. The bold-faced text of the matched lines are matched for regular expression groups, and can be referenced with regular expression group match variables.

Auto-remediation variables can only be accessed within a `@foreach` loop. Because each pattern line can possibly match multiple configuration lines, matched lines are iterated within a loop. To access the above two lines that are matched to the first pattern line of Condition A, use the `@foreach` loop syntax:

```
@foreach $matching_line$ in $condition_A_line_1$
   ...
@end
```

The above line means: Access each matched configuration line that is placed into the array variable (pattern line match variable) of `$condition_A_line_1$` using the `$matching_line$` loop variable.

With the `$matching_line$` loop variable, Auto-remediation scripts can access one matched line in each iteration of the loop. A matched line and its parts for regular expression groups are accessed through the loop variable as follows (in the above `@foreach` loop):

```
$matching_line.regex_group_0$
$matching_line.regex_group_1$
$matching_line.regex_group_2$
```

The variable for group zero (`$matching_line.regex_group_0$`) holds the entire matched configuration line, while others (groups one and two) hold the regular expression groups defined within parentheses. As a result, the values for the variables in the first iteration of the loop are as follows:

```
$matching_line.regex_group_0$: access-list 139 deny  ip host 192.168.139.1 any
$matching_line.regex_group_1$: 139
$matching_line.regex_group_2$: 192.168.139.1
```

As an example, assume the following Auto-remediation script corrects the violations:

```
@foreach $matching_line$ in $condition_A_line_1$
    no $matching_line.regex_group_0$
    access-list 100 permit $matching_line.regex_group_2$ any
@end
```

Each line within the `@foreach` loop is a command to be run on the device. In this example, the first line (`no <line>`) removes a line from the configuration text of the device, while the second line inserts a line into the configuration text of the device.

Note that two variable references are used in the sample Auto-remediation script: `$matching_line.regex_group_0$` and `$matching_line.regex_group_2$`. When this Auto-remediation script is executed by the Policy Manager after a compliance check, the following command script will be generated and scheduled to run on the device:

```
no access-list 139 deny ip host 192.168.139.1 any
access-list 100 permit 192.168.139.1
no access-list 139 deny ip host 192.168.139.2 any
access-list 100 permit 192.168.139.2
```

Example 3: Blocks

Block-based conditions must have nested loops to iterate over the blocks and matches of condition patterns. Assume the following Policy Rule definition includes block start/end patterns and one block text condition:

```
Configuration text:
     ...
      interface Ethernet0/0
       description New York LAN Back Bone
       ip address 10.16.241.1 255.255.255.224
       no ip mroute-cache
       half-duplex
      !
      interface Ethernet0/1
       description Chicago LAN Back Bone
       ip address 10.1.1.1 255.255.255.252
       half-duplex
      !
     ...

Block Start: interface (.*)
Block End:   !

Condition A: Config Block
must not contain
  ip address (10\..*)\s(.*)
```

The `@foreach` loop used to access the violation data of the above condition looks like:

```
@foreach $matching_line$ in $condition_A_line_1$
    no $matching_line.regex_group_0$
@end
```

However, matches for Condition A are organized by blocks. The above `@foreach` loop does not know which block the `$condition_A_line_1$` array has matches. As a result, the condition pattern needs to be surrounded by a `@foreach` loop for the blocks as follows:

```
@foreach $matching_block$ in $block_start$
  @foreach $matching_line$ in $condition_A_line_1$
      interface $matching_block.regex_group_1$
      no $matching_line.regex_group_0$
  @end
@end
```

The generated command script is as follows:

```
interface Ethernet0/0
no ip address 10.16.241.1 255.255.255.224
interface Ethernet0/1
no ip address 10.1.1.1 255.255.255.252
```

Example 4: Must Contain Only Operator

The “Must Contain Only” operator has two patterns:

- The first pattern defines what configuration text must be included.
- The second pattern defines what configuration text must not have other than the matches of the first one.

The violation data is generated for the second pattern. For example:

```
Condition A: Config Text
must contain only:
  Must contain these lines:
    ntp server 169\.243\.103\.34
    ntp server 170\.242\.62\.16
    ntp server 170\.242\.62\.17
    ntp server 169\.243\.226\.94
  But must not have any additional lines containing:
     ntp server(.*)
```

There are two possible violations:

1. Any lines in the “Must contain these lines” patterns do not match against the configuration text. In this case, there is no violation data produced since the violation is due to the absence of the desired lines.
2. Any configuration text line that matches the `ntp server(.*)` pattern does not match any lines in the “Must contain these lines” patterns. In this case, there is violation data. It can be accessed via `$condition_A_line_1$ array` variable.

An Auto-remediation script to correct possible violations might look like the following:

```
ntp server 169.243.103.34
ntp server 170.242.62.16
ntp server 170.242.62.17
ntp server 169.243.226.94

@foreach $matching_line$ in $condition_A_line_1$
  no ntp server $matching_line.regex_group_1$
@end
```

The first four lines ensure that the configuration text has the lines defined in the "Must contain these lines" patterns. The `@foreach` loop is to remove any lines that match the `ntp server(.*)` that caused a violation.

Example 5: @ifexists statement

A regular expression can include groups that might not have any matching text. As a result, variables that reference these groups might have no stored values, for example:

```
logging ((10\.1\..*)|(172\.1\..*))
```

Regular expression groups:

```
Group 0: logging ((10\.1\..*)|(172\.1\..*))
Group 1: ((10\.1\..*)|(172\.1\..*))
Group 2: (10\.1\..*)
Group 3: (172\.1\..*)
```

One of the regular expressions capturing groups for the IP Addresses for Group 2 or 3 will not have any value.

Assume we have the following condition with the above regular expression pattern:

```
Condition A: Config Text
must not contain
  logging ((10\.1\..*)|(172\.1\..*))
```

An Auto-remediation script to access the violation data above must use the `@ifexists` statement to test whether there is any violation data available for the capturing group variables for Groups 2 and 3. Otherwise, no command script is generated when the Auto-remediation script tries to access a capturing group variable that does not have any value.

The Auto-remediation script will look like the following:

```
@foreach $matching_line$ in $condition_A_line_1$
  @ifexists $matching_line.regex_group_2$
    no logging $matching_line.regex_group_2$
  @end
  @ifexists $matching_line.regex_group_3$
    no logging $matching_line.regex_group_3$
  @end
@end
```

Example 6: Multiple Conditions

The following example illustrates multiple conditions.

```
Block Start: interface (.*)
Block End:   !

Condition A: Config Block
must not contain
  ip address (10\..*)\s(.*)

Condition B: Config Text
must contain only:
  Must contain these lines:
    ntp server 169\.243\.103\.34
    ntp server 170\.242\.62\.16
    ntp server 170\.242\.62\.17
    ntp server 169\.243\.226\.94

But must not have any additional lines containing:
  ntp server(.*)

Logic: A AND B
```

The Auto-remediation script will look like the following:

```
@foreach $matching_block$ in $block_start$
  @foreach $matching_line$ in $condition_A_line_1$
      interface $matching_block.regex_group_1$
      no $matching_line.regex_group_0$
  @end
@end

ntp server 169.243.103.34
ntp server 170.242.62.16
ntp server 170.242.62.17
ntp server 169.243.226.94

@foreach $matching_line$ in $condition_B_line_1$
  no ntp server $matching_line.regex_group_1$
@end
```

Running Command Scripts

Your ability to run and to edit instances of command scripts is restricted by your permissions. Users with Limited permissions and Full or Power users who do not have the Modify Device permission cannot run scripts.

You can set up a script to run once, periodically based on a user-defined interval, or as a recurring task. In addition, you can schedule the task to start at a specific time or as soon as possible. Keep in mind that you can edit the script and supply values for variables before running it.

To run a script from the Command Scripts page:

1. On the menu bar under Devices, select Device Tools and click Command Scripts. The Command Scripts page opens.
2. Select the name of the script you want to run.
3. In the Action column, click Run. The Run Command Script Task page opens. Refer to "Run Command Script Task Page Fields" on page 306 for information.

Note: You can also run a command script from the Tasks menu.

Creating a Script from a Configuration Template

To create a script from a configuration template:

1. On the menu bar under Devices, select Device Tools and click Configuration Templates. The Configuration Templates page opens. Refer to "Configuration Templates Page Fields" on page 569.
2. Click the vendor link. The Configuration Templates page for that vendor opens.
3. Select the configuration template to include in your script and click Update Script.
4. Edit the script, if necessary, and click the Create Script button to create a script that can be deployed to the device. The Save Script from Template page opens.
5. Edit the Name, Description, and any other fields. Keep in mind that variable names cannot begin with "tc_". However, they can include any combination of uppercase alpha, lowercase alpha, 0 through 9, and underscore characters.
6. Click Save Script. The Command Scripts page opens. The new script is highlighted.

Chapter 16: Reports

Use the following table to quickly locate information.

Report	Refer to:
Getting Started	"Getting Started" on page 598
User & System Reports	"User & System Reports" on page 599
Network Status Report	"Network Status Report" on page 602
Best Practices Report	"Best Practices Report" on page 605
Device Status Report	"Device Status Report" on page 607
Statistics Dashboard	"Statistics Dashboard" on page 608
Diagramming	"Diagramming" on page 609
Device Software Report	"Device Software Report" on page 618
Software Level Report	"Software Level Report Fields" on page 620
Software Vulnerability Report	"Software Vulnerability Report" on page 622
Image Synchronization Report	"Image Synchronization Report Fields" on page 624
System & Network Events Report	"System & Network Events Report" on page 625
Software Vulnerabilities Event Details Report	"Software Vulnerabilities Event Details Report" on page 626
Summary Reports	"Summary Reports" on page 627
Emailing Reports	"Emailing Reports" on page 630

Getting Started

HP Network Automation (NA) offers both default reports that require no input and ad-hoc reports. Default reports include:

- User and System Reports
- Dashboard reports
- Summary reports
- Best Practices reports
- Network Status reports
- Configuration reports
- Device Status reports
- Software Vulnerability reports
- Task/Job reports
- Telnet/SSH User Session Log reports
- Compliance Center reports

Ad-hoc reports provide flexibility and control to report on data within NA. Ad-hoc reports can be manually or automatically generated based on regular expression criteria for one or more fields. Common ad-hoc reports could include:

- All Cisco devices running 12.* versions of IOS
- All devices using insecure protocols for configuration management
- All devices with a faulty module
- All configuration changes made over a period of time for a set of devices
- All Telnet/SSH session logs initiated by a specific user
- All device changes that results because of an approval override
- All ACLs that deny traffic on specific ports

User & System Reports

The User & System reports are the results of searches you defined and saved using the Search capabilities. Only searches for which you defined appear in the list of User reports. You can search for:

- Devices
- Interfaces
- Modules
- Configurations
- Diagnostics
- Policies
- Compliance
- Tasks
- Sessions
- Events
- Users
- ACLs
- IP addresses
- MAC addresses
- VLANs

For information on performing searches, refer to "Searching for Devices" on page 474.

Each report includes a summary of the criteria used in the search. Your saved searches are not available to anyone but you and the NA Administrator.

Note: If you have not run and saved any searches, no User reports are available.

System reports on pre-defined queries. They are generated when you select the report. Each report includes a summary of the criteria used in the search. The System reports include:

Configuration	• All changes made in the last 12 hours • All changes made in the last 24 hours • All changes made in the last 48 hours • All changes made in the last week • All changes made in the last month • All changes made by myself in the last 48 hours
Policy Events	Policy rule violations in the past 24 hours.

Devices	• All devices changed in the last 24 hours • All devices changed in the last week • All devices with access failures • All inactive devices (Note: Rather than deleting inactive devices, you can specify them as inactive so as to retain the configuration history.) • All duplicate IP addresses • All devices without driver assigned • All devices with driver assigned but no configuration stored • All devices with different startup and running configurations
Duplicate IP	All duplicate IP addresses — This report displays which devices have interfaces that are configured with the same IP address. However, it does not remove the IP address that is causing the duplicate detection. The IP type is either how the IP address was added or how it is used. The values for this column are: 1 — Manual (A manually added IP address.) 2 — NAT (Network Address Translation, user-defined NATed IP address.) 3 — Primary on Port (Primary IP address for a port.) 4 — Secondary on Port (Secondary IP address for a port.) 5 — TFTP to Device (IP address to access a device via TFTP.) 6 — Primary on Device (Primary IP address used to access the device.) 7 — Console (IP address for console access to the device.)
Session	• All sessions created in the last 24 hours • All sessions created in the last 48 hours • All sessions created in the last week • All sessions created by myself in the last 48 hours
Software Levels	• Device Software Levels
Task	• All failed, skipped, and duplicate tasks in the last 24 hours • All failed, skipped, and duplicate tasks in the last week

Other	• Best Practices Report • Network Status Report • Device Status Report • COSO Compliance Status • COBIT Compliance Status • GLBA Compliance Status

To view the User & System reports, on the menu bar under Reports click User & System Reports. The User & System Reports page opens.

User & System Reports Fields

Field	Description/Action
Type	Displays the type of event or report.
Report	Displays the name of the report, for example Device Status, HIPAA Compliance Status, All inactive devices, and so on. Clicking the report opens the report.
Actions	You can select the following actions: • Email Report — Displays the Email Report form where you can create a task to send the output of a report via email. You can specify the recipient. User login is the default. You must save the task to generate the email message. • Modify — For User reports, you can click the Modify option for an event. The Search For Events page opens. • Mark as System Report — For User reports, you can click the Mark as System Report. The report is moved to the System Reports section. • Delete (red X icon) — Permanently deletes the report. • Click the Up or Down arrows to move the report up or down in the list.

Network Status Report

The Network Status Report provides an overview of network configuration, health, and compliance, combined with two independent views of the network:

- Best Practices
- Device Status

The Network Status report delivers proactive reporting capability. By scheduling the report to run as a recurring Email Report task, network administrators and engineers automatically receive up-to-date information that can help eliminate problems before they impact the network. Network Status reports can also provide management with an overview of network operations' effectiveness in resolving policy and software level issues and handling configuration changes.

Note: The default configuration for this report is to run against the Inventory device group.

Events are reported based on a three-tiered representation of the risk introduced to the network. The System Administrator sets the threshold for each category and assigns the risk level indicator color to reflect the impact on the network.

- Red — High risk, including policy violations, software level violations, and device access failures combined with any other Yellow level event.
- Yellow — Moderate risk, including startup and running configuration mismatches and device access failures.
- Green — Within threshold or low risk. This is the best practice.

The status of any device group is based on the highest risk condition of any device in the group. The status of the network is based on the highest risk condition of any group in the network.

To view the Network Status report, on the menu bar under Reports, click Network Status. You can run this report on demand using the Run Again button on the report page or schedule the report to run as a task and email it to key network and management staff using the Email Report option. For information on emailing reports, refer to "Emailing Reports" on page 630.

Network Status Report Fields

Field	Description/Action
Best Practices Report link	Opens the Best Practices Report. Refer to "Best Practices Report" on page 605.
Device Status Report link	Opens the Device Status Report. Refer to "Device Status Report" on page 607.
Report Date	Displays the date and time the report was last run.
Device Groups Reported	Displays the number of reported device groups.

Field	Description/Action
Change Device Groups	Displays a list of currently defined device groups. You can run the Network Status report for a single device group or for multiple devices groups. All other parameters are pre-defined. Summary and detail information is provided per category for each device group you specify. Click the Run Again button when finished.
Status	Displays the name of the device group and the number of devices in the group.
Device Status	
Device Status	Displays the status level indicator with percentages of issues found. Status levels include: • Red — High risk • Yellow — Moderate risk • Green — Low risk If you click Device Status, the Device Status report opens. Refer to "Device Status Report" on page 607.
Best Practices Status	
Issue	Displays the five key network issues that NA tracks, including: • Policy Rule Violations — Devices that do not comply with one or more defined configuration policies. Move the cursor over the information icon for more information. • Software Level Violations within 24 hours — Devices that are running non-approved software versions. Move the cursor over the information icon for more information. • Startup vs. Running Configuration Mismatch — Devices with mismatched startup and running configurations. Move the cursor over the information icon for more information. • Device Access Failure — Devices that NA could not reach. Move the cursor over the information icon for more information. • Configuration Changes within 24 hours — Device configuration changes detected in the past 24 hours. Move the cursor over the information icon for more information. Available action links vary for each issue. For example, for all reported Device Access Failures, you can click the link to view the device details View Task option, where you can identify the tasks that failed. For Startup vs. Running Configuration Mismatches, you can click the link to view the Compare Startup with Running option, which shows both configurations with the differences highlighted. If you click Best Practices Status, the Best Practices report opens. Refer to "Best Practices Report" on page 605.

Field	Description/Action
Network Status Report Details	
High Risk (Red) Issues	Displays summary information for any of the five issues that returned a red status. Available action links vary for each issue. For example: • All reported Device Access Failures — Click the link to view the device details View Task option, where you can identify the tasks that failed. • Policy Rule Violations — Click the link to view the Configuration Policy Activity page, where you can view events that show if a device's configuration was not in compliance with the configuration rules contained in one or more configuration policies. The value shown in the Policy Importance column is the highest importance of all configuration rules currently violated by the device. • Startup vs. Running Configuration Mismatches — Click the link to view the Compare Startup with Running option that shows both configurations. All differences are highlighted.

Best Practices Report

Best practices for network management dictate that non-compliance with any of the following issues be carefully monitored:

- Policy Rule Violations within 24 hours
- Software Level Violations
- Startup vs. Running Configuration Mismatch
- Device Access Failure
- Configuration Changes within 24 hours

NA enables you to define the acceptable level of non-conformance with each of these issues. If the threshold is exceeded, a yellow or red warning is shown depending on the level of non-compliance. NA also displays which devices failed to comply so you can take corrective action.

If all five indicators are green, NA has evaluated your network and determined your network health is good. If some indicators show yellow, you should target those areas for corrective action. If some indicators are red, the issues flagged could represent a critical risk to network stability and should receive immediate attention.

To view the Best Practices report, on the menu bar under Reports click Best Practices. The Best Practices report opens.

Note: You can also navigate to the Best Practices report from the Network Status report.

Best Practices Report Fields

Field	Description/Action
Network Status Report link	Opens the Network Status report. Refer to "Network Status Report" on page 602.
Device Status Report link	Open the Device Status Report. Refer to "Device Status Report" on page 607.
Report Date	Displays the date and time the report was last run.
Device Groups Reported	Displays the number of reported device groups.
Change Device Groups	Displays a list of currently defined groups. You can run the Best Practices report for a single group or for multiple groups. All other parameters are pre-defined. Summary and detail information is provided per category for each group you specify. Click the Run Again button when finished.
Status	Displays the name of the group and the number of devices in the group. Status levels include: • Red — High risk • Yellow — Moderate risk • Green — Within threshold
Issue	Displays the five key network issues that NA tracks, including: • Policy Rule Violations within 24 hours — Devices that do not comply with one or more defined configuration polices. Move the cursor over the information icon for more information. • Software Level Violations — Devices that are running non-approved software versions. Move the cursor over the information icon for more information. • Startup vs. Running Configuration Mismatch — Devices with mismatch startup and running configurations. Move the cursor over the information icon for more information. • Device Access Failure — Devices that NA could not reach. Move the cursor over the information icon for more information. • Configuration Changes within 24 hours — Device configuration changes detected in the past 24 hours. Move the cursor over the information icon for more information.
Best Practices Report Details	
High Risk (Red) Issues	Displays summary information for any of the five issues that returned a red status. Available action links vary for each issue. For example, for all reported Device Access Failures, you can click the link to view the device details View Task option, where you can identify the tasks that failed. For Startup vs. Running Configuration Mismatches, you can click the link to view the Compare Startup with Running option that shows both configurations. All differences are highlighted.

Device Status Report

The Device Status report lists all of the devices in your network and analyzes them individually for each of the Best Practices issues. Refer to "Network Status Report Fields" on page 602 for information on each of the Best Practices issues.

Each device that does not comply with one or more of the issues is flagged with a yellow or red warning. The report also summarizes the entire network to see how many devices generated yellow or red warnings.

To view the Device Status report, on the menu bar under Reports click Device Status. The Device Status report opens.

Note: You can also navigate to the Device Status report from either the Network Status report or the Best Practices report.

Device Status Report Fields

Field	Description/Action
Network Status Report link	Opens the Network Status report. Refer to "Network Status Report" on page 602.
Best Practices Report link	Opens the Best Practices Report. Refer to "Best Practices Report" on page 605.
Report Date	Displays the date and time the report was last run.
Device Groups Reported	Displays the number of reported device groups.
Change Device Groups	Displays a list of currently defined groups. You can run the Best Practices report for a single group or for multiple groups. All other parameters are pre-defined. Summary and detail information is provided per category for each group you specify. Click the Run Again button when finished.
Status	Displays the name of the group and the number of devices in the group. Status levels include: • Red — High risk • Yellow — Moderate risk • Green — Within threshold
Device Status Report Details	
Moderate Risk (Yellow) and High Risk (Red) Issues	Displays summary information for any of the five issues that returned a yellow or red status. Available action links vary for each issue. For example, for all reported Config Changes within 24 hours, you can click the View Config link to view the configuration information for that decide. For Device Access Failures, you can click the View Device Tasks link, where you can identify the tasks that failed.

Statistics Dashboard

To view the Statistics Dashboard, on the menu bar under reports, click Statistics Dashboard. The Statistics Dashboard opens. The Statistics Dashboard provides information on the following reports:

- Top 5 Vendors — Refer to "Summary Reports" on page 627 for information.
- Top 5 OS Versions — Refer to "Summary Reports" on page 627 for information.
- Number of Configuration Change - Last 7 Days — Refer to "User & System Reports" on page 599 for information.
- Change History by Time of Day — Refer to "Summary Reports" on page 627 for information.
- Top 10 Most Accessed Devices — Refer to "Summary Reports" on page 627 for information.
- System Status — Refer to "Network Status Report" on page 602 for information.
- Software Level — Refer to "Summary Reports" on page 627 for information.
- Configuration Policy Compliance — Refer to "Summary Reports" on page 627 for information.

Diagramming

Diagramming enables you to gather topology data from your network devices. Network diagrams can be viewed in either Visio, static JPEG, or interactive JPEG format and printed. The topology data, including Layer 3 IP addresses and subnets, and Layer 2 details spanning MAC addresses and VLANs, provides a snapshot of the current state of your network.

Diagramming must be enabled on the **Admin > Administrative Settings > Reports** page. For more information, see "Diagramming" on page 73.

In terms of VLANs, the ports associated with a given VLAN are drawn in the VLAN box. Cisco's VLAN Trunking Protocol (VTP) Domain information is also displayed, if applicable. All aggregated ports are hidden, with an annotation to the associated port channel that lists the aggregated port names. Refer to "Virtual Local Area Networks (VLANs)" on page 215 for detailed information on VLANs.

Keep in mind that Layer 3 data includes IP addresses obtained from the device's configuration file. Layer 2 data is tied to the MAC addresses of the interfaces on each device and data from the MAC tables showing what MAC address the device sees. NA maps which devices can communicate with each other as a result of being on the same network.

You can detect Layer 1 (physical cable) connections. Layer 1 connections are inferred from Layer 2 data (MAC addresses that are seen by switches), captured, and then added to the NA database. The Layer 1 diagram type in NA displays the same connections as in HP SA. Refer to the *HP Server Automation User's Guide* for information.

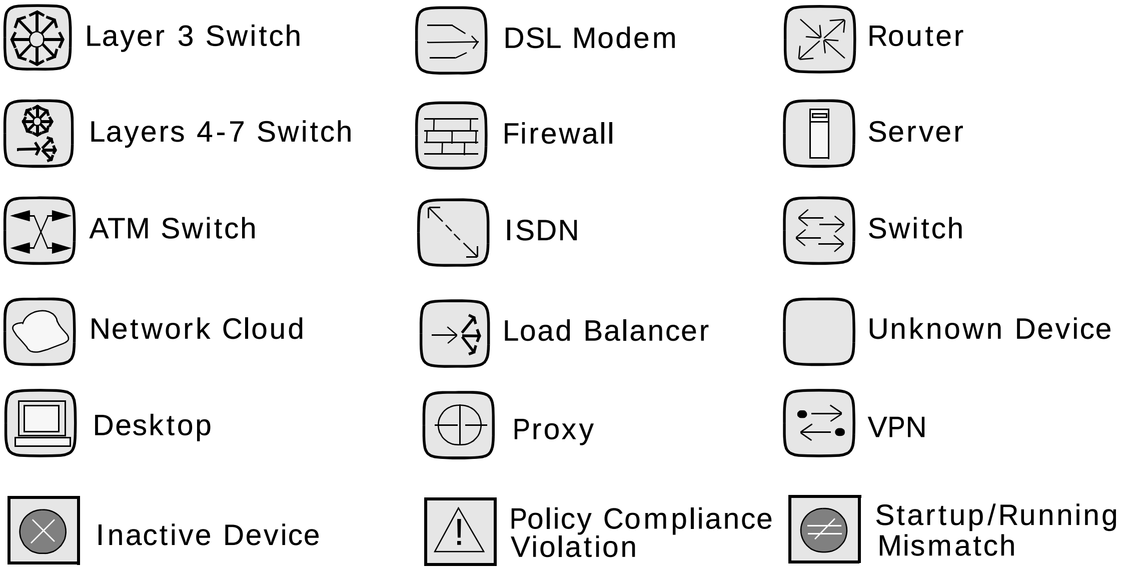
The inferred Layer 1 data is based on heuristics. NA reduces the number of data link connections between devices and/or servers to make network diagrams more readable. Only connections that can be inferred through transitive connections are reduced.

In the OSI model, each layer is an abstraction designed to hide the layer below. Therefore, the Layer 2 data gathered from devices cannot generate 100% accurate Layer 1 data. In particular, Layer 1 data could be incorrect if any of the following conditions exist:

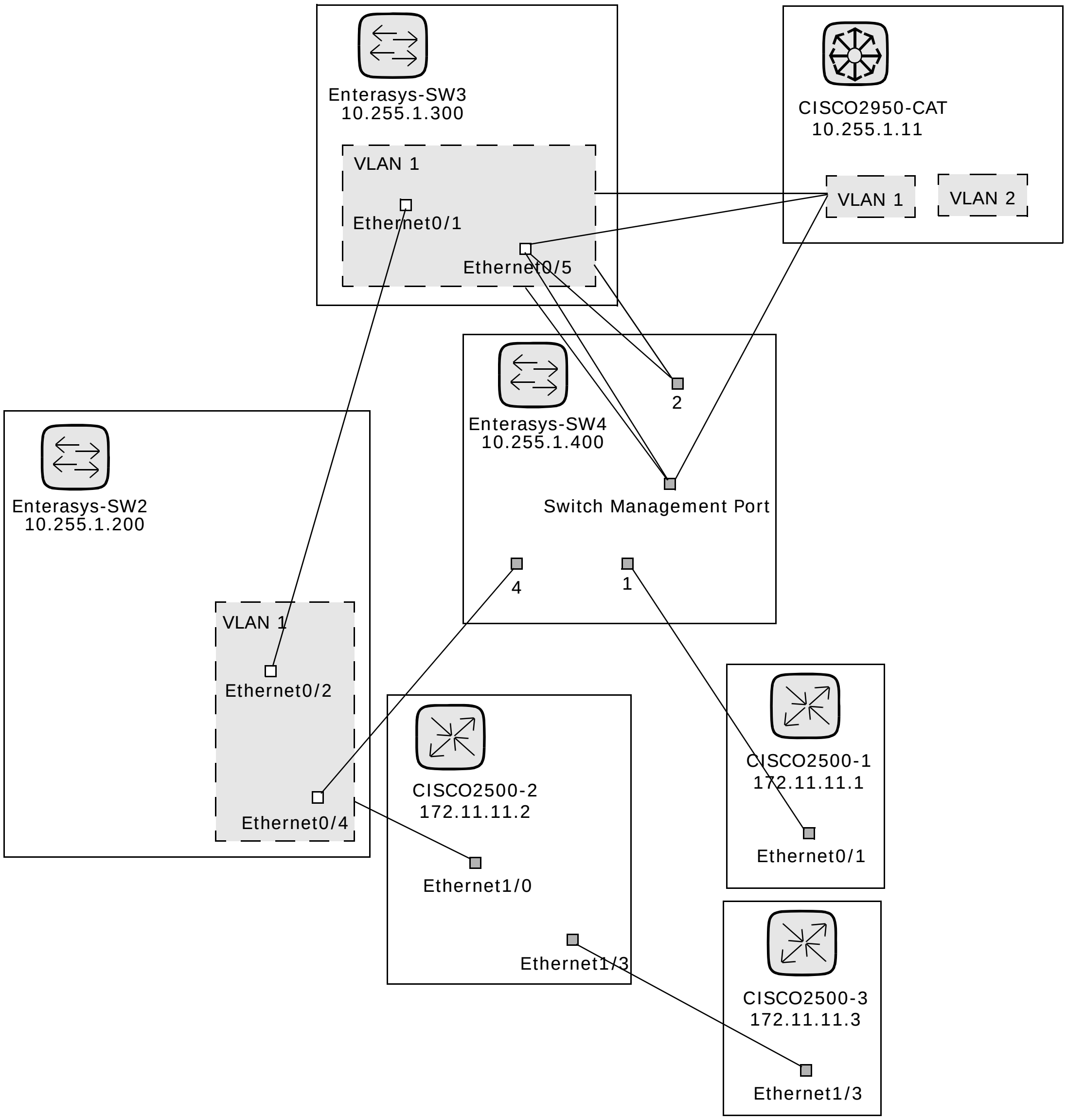
- The device does not return the interface number where MAC addresses are seen.
- There was no traffic between the devices within a few minutes of when NA gathers the topology data (where MAC addresses are seen).
- There is an unaddressable device, such as a hub, between two managed devices.

The following colors, borders, lines, and icons are used in diagrams.

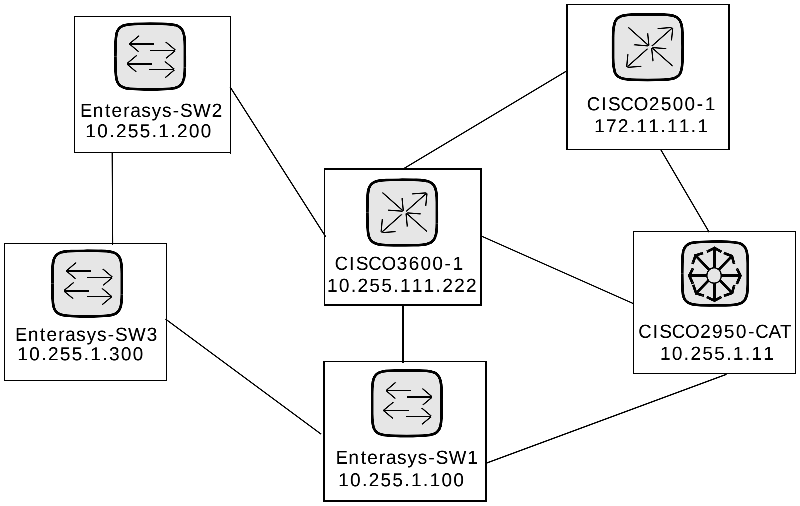
- Red — The device failed its last access, either as a result of a Snapshot task or another task. (**Note**: For VLANs and ports, red indicates that the VLAN is administratively down and gray indicates that the VLAN is up and running.)
- Gray — The device contains no snapshot data.
- White — The device is up and running.
- Device borders — A solid border indicates a device. A dashed border indicates a virtual grouping, where each VLAN in a device is shown as its own device.
- Dashed lines — Depict Layer 3 connections.
- Solid lines — Depict Layer 2 connections.


Layer 3 Switch
DSL Modem
Router
Layers 4-7 Switch
Firewall
Server
ATM Switch
ISDN
Switch
Network Cloud
Load Balancer
Unknown Device
Desktop
Proxy
VPN
Inactive Device
Policy Compliance Violation
Startup/Running Mismatch

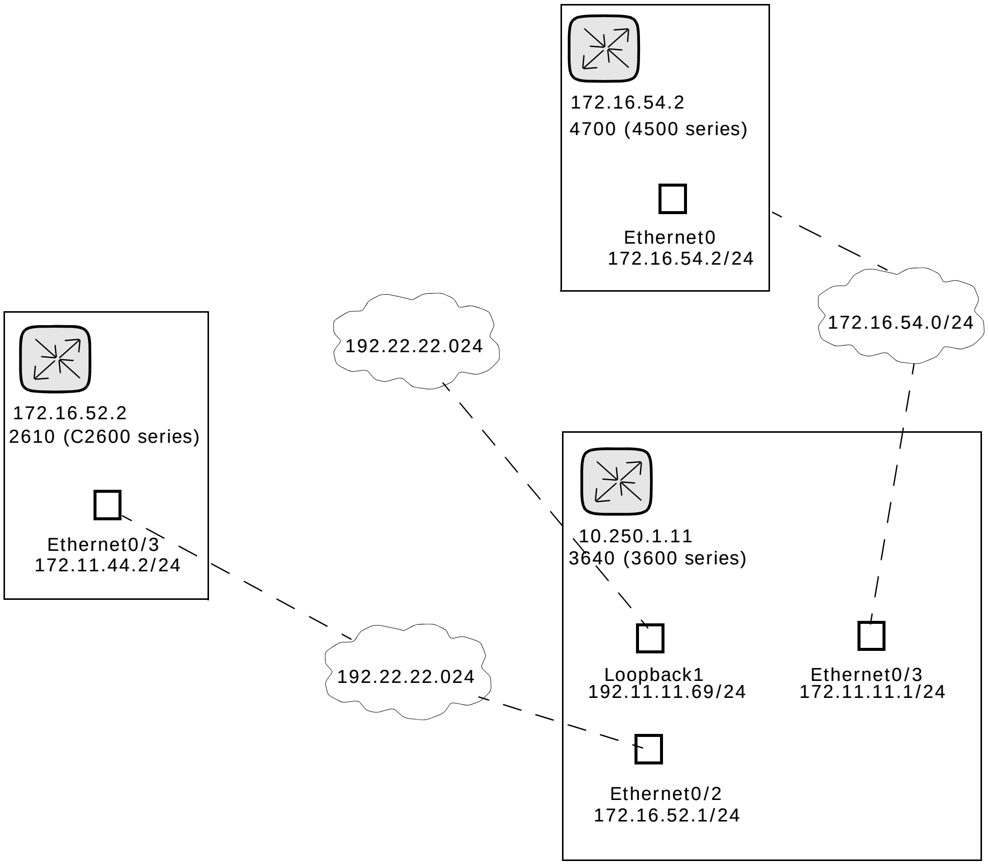
The following figure shows a simple network diagram, including connections between VLANs and ports.


Enterasys-SW3
10.255.1.300
VLAN 1
Ethernet0/1
Ethernet0/5
CISCO2950-CAT
10.255.1.11
VLAN 1
VLAN 2
Enterasys-SW4
10.255.1.400
2
Switch Management Port
4
1
Enterasys-SW2
10.255.1.200
VLAN 1
Ethernet0/2
Ethernet0/4
CISCO2500-2
172.11.11.2
Ethernet1/0
Ethernet1/3
CISCO2500-1
172.11.11.1
Ethernet0/1
CISCO2500-3
172.11.11.3
Ethernet1/3

The following sample figure shows a simple network diagram with collapsed devices.


Enterasys-SW2
10.255.1.200
CISCO2500-1
172.11.11.1
CISCO3600-1
10.255.111.222
Enterasys-SW3
10.255.1.300
CISCO2950-CAT
10.255.1.11
Enterasys-SW1
10.255.1.100

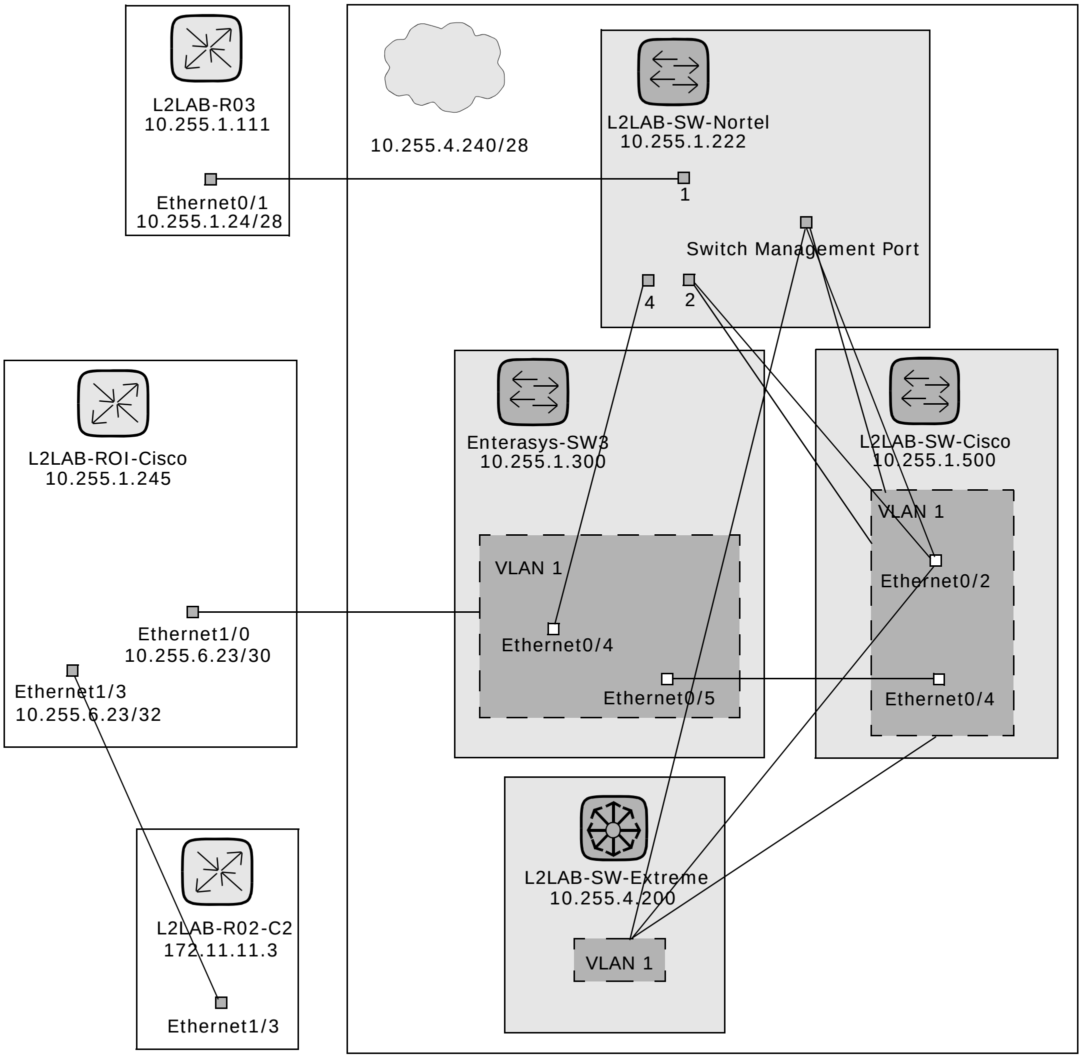
The following sample figure shows a simple network diagram utilizing clouds as a shortcut method to connect devices that share the same subnet. Keep in mind clouds can logically represent gateway objects, such as routers and switches.


172.16.54.2
4700 (4500 series)
Ethernet0
172.16.54.2/24
172.16.54.0/24
192.22.22.024
172.16.52.2
2610 (C2600 series)
Ethernet0/3
172.11.44.2/24
10.250.1.11
3640 (3600 series)
Loopback1
192.11.11.69/24
Ethernet0/3
172.11.11.1/24
192.22.22.024
Ethernet0/2
172.16.52.1/24

A Layer 3 diagram collects all selected devices and connects the devices in the same subnet using the IP address and subnet mask. Multiple devices in a subnet are connected with a cloud. As a result, the cloud represents the subnet.

An expanded Layer 3 diagram starts with a basic Layer 3 diagram. If more than one device is connected to a subnet, the subnet is expanded to locate all the devices that might lie within the subnet. Expanded Layer 3 diagrams include all the interfaces connected to the cloud and traverse to other devices via known Layer 2 connections (discovered from the Topology Gathering diagnostic). The expanded cloud then becomes a container for all devices that participate in the subnet. Keep in mind that as Layer 2 connections are traversed, devices could be added to the diagram that were not originally selected.

The following sample figure shows an expanded Layer 3 network diagram. After the basic Layer 3 diagram is generated, each cloud that has more than one device connected to it is expanded. Keep in mind that NA walks all of the Layer 2 connections. As a result, the devices in the cloud are grouped within a cloud node.


L2LAB-R03
10.255.1.111
Ethernet0/1
10.255.1.24/28
10.255.4.240/28
L2LAB-SW-Nortel
10.255.1.222
1
Switch Management Port
4
2
L2LAB-ROI-Cisco
10.255.1.245
Ethernet1/0
10.255.6.23/30
Ethernet1/3
10.255.6.23/32
Enterasys-SW3
10.255.1.300
VLAN 1
Ethernet0/4
Ethernet0/5
L2LAB-SW-Cisco
10.255.1.500
VLAN 1
Ethernet0/2
Ethernet0/4
L2LAB-SW-Extreme
10.255.4.200
VLAN 1
L2LAB-R02-C2
172.11.11.3
Ethernet1/3

To view the Diagramming page, on the menu bar under Reports click Diagramming. The Diagramming page opens. When you are done configuring your diagram, click the Generate button.

Diagramming Page Fields

Field	Description/Action
Diagram Type	Select one of the following diagram types from the drop-down menu. A sample diagram indicating the type of diagram is displayed to the right of the drop-down menu. • Layer 1: Ports (Inferred) • Layer 2: Ports • Layer 3: Ports • Layer 3: Ports (Expanded) • Layer 1: Devices (Inferred) • Layer 2: Devices • Layer 3: Devices • Layer 3: Devices (Expanded) **Note**: The inferred Layer 1 data is based on heuristics. NA reduces the number of data link connections between devices and/or servers to make network diagrams more readable. Only connections that can be inferred through transitive connections are reduced. Refer to "NA/SA Integration" on page 198 for more information.
Output format	Select one of the following formats for your network diagram: • JPEG (Interactive) — Enables you to display your network diagram in Joint Photographic Experts Group (JPEG) output and select devices in the network diagram. When you select a device, the Device Details page opens for the device. (Refer to "View Menu Options" on page 203.) • JPEG (Static) — Displays your network diagram in Joint Photographic Experts Group (JPEG) format. • Visio — You must have Visio 2003 or higher, including Service Pack 2 or higher, or the Visio Viewer installed on your system for viewing network diagrams in Visio. These are .rdx files.
Device Selection	Select one of the following options: • Devices & Groups — Enter an IP Address, Hostname, or Device Group name on which to run the task against or click the magnifying glass icon. For information on how to use the Device Selector, refer to "Device Selector" on page 144. • Route — Enter a starting route device and an end route device. NA runs an ICMP Test task between the two devices. (Refer to "Run ICMP Test Task Page Fields" on page 301 for information on the ICMP Test task.) This is done as a traceroute, which shows all of the IP addresses that were encountered between the source device and the destination device. • Single Device — Enter the IP address or hostname of the device. You can designate the number of connections to display up to three hops.

Field	Description/Action
Hierarchy Layer Filter	A hierarchy layer is a device attribute. You can set a device's hierarchy layer when adding or editing a device. (Refer to "Adding Devices" on page 108 for information.) As a result, when configuring a diagram, you can select a hierarchy layer on which to filter. For example, you could diagram your entire network (Inventory) and then filter on "Core" to diagram only your Core devices—devices with a hierarchy layer set to Core. **Note**: The options provided below are default filters. You must assign filtering values to your devices to be able to designate a filter here. Refer to "Editing the appserver.rcx file" on page 617 for information on creating custom filters. Select one or more of the following options from the drop-down menu: • Core • Distribution • Access • Edge
Advanced Options	
Advanced Filter	Select one or more of the following options: • Hide inactive devices — Removes all inactive devices from the network diagram. • Hide devices not connected to any other selected devices — Removes all devices that have no connections to other devices from the network diagram. • Hide VLANs that have no connections — Removes VLANs that are not connected to any ports or other VLANs from the network diagram. • Hide unconnected interfaces/ports — Removes all interfaces and ports that have no connections to other devices from the network diagram. • Hide ports not associated with a device — Removes all Layer 2 ports not associated with a device from the network diagram. (**Note**: NA collects routing information from each managed device. Often times, devices have routes to devices and ports that are connected to non-managed devices. A device could see a port that is on a NA managed device, but that device may not support the NA Topology Data Gathering diagnostic. In this case, NA cannot make the grouping connection between the port and the device.) • Enter the minimum number of subnet connections to create a subnet cloud. The default is 2.
Grouping	Select one or both of the following options: • Connect contained subnets to their supernet — Enables you to group subnets together. For example, presume IP address range 10.255.0.0/23 and the range 10.255.1.0/24. The /24 network is contained within the /23 network. It is possible that traffic can flow between the two network. As a result, the /23 network and the /24 network would be shown as connected in the diagram. • Show VLANs as separate devices — Separates a device into multiple representations of the same device (one for each VLAN). VLAN devices are shown with a dashed outline, the same as the VLAN grouping within devices for the other graph types. (**Note**: This option is automatically selected for Expanded L3 diagrams and cannot be disabled.)

Field	Description/Action
Annotations	
Device Annotations	Select the fields you want to appear with each graphed device. Keep in mind that it does not take too many fields for the graph to become overwhelmed with text. Some of the available options include: • Hostname • Primary IP • Fully Qualified Domain Name • Device Description • Partition • Model • Vendor • Serial Number • Asset tag • Last Changed Date • Custom Fields • Last Access Status • Show Device Inactive • Show Policy Compliance Status • Show Startup/Running Mismatch • VTP Information
Endpoint Annotations	Select one or more of the following options: • Interface Description • Port Name • IP Address • Port Type • Port Status • Running Port State • MAC Address • Realm
Interconnection Annotations	Select one or more of the following option: • Subnet — Labels the interconnecting lines with subnet information. • VLAN — Labels the interconnecting lines with VLAN information.
Cloud Annotations	Select the following option: • Subnet — Text is included with a Layer 3 cloud (a shortcut method to connect devices that share the same subnet). • Realm — Text is included with a Layer 3 cloud. (A Realm is a network segment with no overlapping IP addresses.)

Field	Description/Action
Graph Annotations	Select the following option: • Annotation Titles — Provides a title for each selected annotation. For example: Hostname: L2LAB-SW01-C0000xl
Save diagram as a user report named:	Enter as name for the diagram and click the Save button.
Email diagram to:	Enter an email address and click the Email button.

Once your diagram has been generated, if you selected the JPEG - Interactive option, clicking a device opens the Device Details page for the device. Refer to "Viewing Device Details" on page 195 for information.

Editing the appserver.rcx file

Hierarchy filtering layers are given values in the order of the their appearance. For example, Core is 1, Distribution is 2, and so on. This information is stored in the appserver.rcx file located in the *Product/config* directory. The file looks like the following:

```
<array name="diagramming/hierarchy_layers">
  <value>core</value>
  <value>distribution</value>
  <value>access</value>
  <value>edge</value>
</array>
```

Keep in mind that the numeric values are stored in the database. If you edit the appserver.rcx file, the changes are not reflected in the database. Consequently, you will also need to change the data associated with the device. (Refer to "New Device Page Fields" on page 108 for information.)

Device Software Report

The Device Software report enables you to view the software version and compliance rating currently assigned to each device.

To view the Device Software report, on the menu bar under Reports, click Device Software. The Device Software Report opens.

Device Software Report Fields

Field	**Description**
Software Level Report link	Opens the Software Level report, where you can view the software versions and levels currently assigned to each device. Refer to “Software Level Report Fields” on page 620.
Software Levels link	Opens the Software Levels page, where you can edit or delete a software level. Refer to “Adding a New Software Level” on page 451.
Current Working Group	Select a device group from the drop-down menu. Inventory is the default.
Level At or Below	Select a software level, for example: • Any Level • Security Risk • Pre-production • Bronze • Silver
Host Name	Displays the hostname of the device. Clicking the hostname opens the Device Details page, where you can view detailed information about the device.
Device IP	Displays the IP address of the device. Devices in red failed the last snapshot attempt. Inactive devices are marked with an icon beside the IP address.
Change Date	Displays when the software was last deployed to the device.
Device Software Version	Displays the detected software version running on the device.
Software Level	Displays the software level, if applicable.
Importance	Displays the severity of the security vulnerability, including: • Informational — Events that typically do not require a response. • Low — Events that may require a response as time permits. • Medium — Events that require a timely response, typically within 72 hours. • High — Events that require an urgent response, typically within 24 hours. • Critical — Events that require an immediate response.
Comments	Provides a description of the vulnerability.

Field	Description
Actions	You can select the following action: • View Software Audit Trail — Opens the Device Software Audit Trail page, where you can view what software is loaded on the device. Refer to “Device Software History Page Fields” on page 230 for information.

Software Level Report

The Software Level report enables you to view the software versions and levels currently assigned to each device.

To view the Software Level report:

1. On the menu bar under Policies, click Software Levels. The Software Levels page opens. Refer to "Software Levels Page Fields" on page 437 for information.
2. Click the Software Level Report link at the top of the page. The Software Level Report opens.

Software Level Report Fields

Field	Description
Device Software Report link	Opens the Device Software report, where you can view the software version and compliance rating currently assigned to each device. Refer to "Device Software Report Fields" on page 618.
Software Levels link	Opens the Software Levels page, where you can edit or delete a software level. Refer to "Adding a New Software Level" on page 451.
Current Working Group	Select a device group from the drop-down menu. Inventory is the default.
Importance At or Above	Select an importance level for the severity of the security vulnerability, including: • Informational — Events that typically do not require a response. • Low — Events that may require a response as time permits. • Medium — Events that require a timely response, typically within 72 hours. • High — Events that require an urgent response, typically within 24 hours. • Critical — Events that require an immediate response.
Host Name	Displays the hostname of the device. Clicking the hostname opens the Device Details page, where you can view detailed information about the device.
Device IP	Displays the IP address of the device. Clicking the IP address opens the Device Details page, where you can view detailed information about the device.
Change Date	Displays the date and time the software was last deployed to the device.
Device Software Version	Displays the detected software version running on the device.
Software Level	Displays the software level rating of the software.

Field	Description
Importance	Displays the severity of the security vulnerability, including: • Informational — Events that typically do not require a response. • Low — Events that may require a response as time permits. • Medium — Events that require a timely response, typically within 72 hours. • High — Events that require an urgent response, typically within 24 hours. • Critical — Events that require an immediate response.
Comments	Provides a detailed description of the vulnerability.
Actions	You can select the following action: • View Software Audit Trail — Opens the Device Software Audit Trail page, where you can view what software is loaded on the device. Refer to "Device Software History Page Fields" on page 230 for information.

Software Vulnerability Report

Unless you have The HP Live Network policies loaded, the Software Vulnerability Report displays an empty search results page.

Note: TON enables you to download Security Alert Service data and other NA Content Service material. For information on HP Live Network, refer to "Help Menu Options" on page 26.

Once you have imported the TON policies and run the compliance check, the results specific to any policy that has a Common Vulnerabilities and Exposures (CVE) value are displayed.

Keep in mind that the Software Vulnerability report gathers data from the tables that contain the results of the compliance and policy checks. As a result, there are no specific software vulnerability events generated. The events generated are policy non-compliance events.

To view the Software Vulnerability report, on the menu bar under Reports, click Software Vulnerabilities. The Software Vulnerability report opens.

Software Vulnerability Report Fields

Field	Description/Action
Check Boxes/Drop-down Menus	You can use the left-side check boxes to selected specific devices. Once you have selected the devices, you can select the Actions drop-down menu select an action, for example: • Batch Edit • Check Policy Compliance • Deploy Passwords • Reboot Device
Host Name	Displays the device's host name.
Device IP	Displays the device's IP address.
Device Compliance State	Displays the device's compliance state.
Policy	Displays the name of the policy.
Rule	Displays the policy configuration rule.
Rule Importance	Displays the importance level, either: • Informational — Events that typically do not require a response. • Low — Events that may require a response as time permits. • Medium — Events that require a timely response, typically within 72 hours. • High — Events that require an urgent response, typically within 24 hours. • Critical — Events that require an immediate response.
Rule Description	Displays the rule description.

Field	Description/Action
CVE	Displays the CVE (Common Vulnerabilities and Exposures) name, along with an operator. CVE is a list of standardized names for vulnerabilities and other information on security exposures.
Last Checked Date	Displays the last checked date.

Image Synchronization Report

The Image Synchronization report enables you to view the currently running or backup software images on a device, or group of devices, that do not reside in the NA software image repository. You can then schedule a task to copy the software images from the device(s) to the NA software image respository. As a result, all software images will be available for download from the NA software repository in the event of an emergency.

Note: Not all device drivers support this functionality. Refer to the Driver Release Service (DRS) documentation for detailed information on supported devices. The DRS is an automated driver release and delivery system.

To view the Image Synchronization report, on the menu bar under Reports, select Image Synchronization Report. The Image Synchronization report opens.

Image Synchronization Report Fields

Field	Description/Action
Current working group	Displays the default group. You can select a different group from the drop-down menu, if applicable.
Check Boxes/Drop-down Menus	You can use the left-side check boxes to selected specific devices. Once you have selected the devices, you can select the Select drop-down menu to click All or None or select the adjacent Actions drop-down menu and click the Sync Image or Exclude Filename option. The Exclude Filename option enables you to add a filename to a list that NA ignores. As a result, the filename is not displayed in the Image Synchronization Report. (**Note**: You must have Modify Device Permission to use the Sync Image option.)
Synch Image option	Opens the Backup Device Software Task page, where you can copy software images to the NA software image repository. (Refer to "Backup Device Software Task Page Fields" on page 371 for information.)
Host Name	Displays the host name of the device. Clicking the Host Name opens the Device Details page, where you can view information about the device and its configuration history.
Device IP	Displays the IP address of the device. Clicking the IP Address opens the Device Details page, where you can view information about the device and its configuration history.
Slot	Displays the slot in which the software image resides on the device.
File Name	Displays the name of the software image.
File Size	Displays the size of the software image.
Email Search Result	Enter the email address to send the search results to and click Send. Be sure to separate multiple email addresses with a comma.
View Search Result as a CSV File link	Opens the search results in CSV format using Excel (Windows platform) or Star Office or Gnumeric (Unix platform).

System & Network Events Report

The System & Network Events report enables you to track events that indicate changes to either a single device or all of your devices. For a complete list of events, refer to "Event Descriptions" on page 520.

To view the System & Network Events report, on the menu bar under Reports click System & Network Events. The System & Network Events report opens.

System & Network Events Report Fields

Field	**Description/Action**
New Message link	Opens the New Message page, where you can post a message to all users referring to this device. You also have the option of tracking the event with SingleView.
For the:	Displays the time frame for viewing events. Options include: • Past 1, 2, 4, 8, 12, 24, and 48 hours • Past 1 and 2 weeks • Past 1 month • All Events
Current Working Group	Select a device group from the drop-down menu.
Check Boxes	You can use the left-side check boxes to delete events from the NA database. Once you have selected the events, click the Actions drop-down menu and click Delete. This deletes the selected events from the NA database. The adjacent Select drop-down menu enables you to select or deselect all of the events.
Event Date	Displays the date/time of the event in the format MMM-dd-yy HH:mm:ss. (The format is configurable by the System Administrator.)
Host Name	Displays the host name or IP address of the device. Clicking the Host Name or IP Address opens the Device Details page, where you can view information about the device and its configuration history.
Summary	Displays the type of event. For a list of Events, refer to "Event Descriptions" on page 520. Clicking the event type link opens the Event Detail page. This page includes: • The date and time the event occurred. • The login name of the person or process that added the event. Clicking the Detail link for diagnostic changes opens the Task Result page where you can view task details. Refer to "Task Information Page Fields" on page 408. • The event type. • A brief description of the event. • A link to detailed information about the device.
Added By	Displays the login name of the person whose action caused the event to be created.

Software Vulnerabilities Event Details Report

The software vulnerabilities event details report enables you to view details about software vulnerability, including advisory information and possible solutions.

To view the Software Vulnerabilities Event details:

1. On the menu bar, select Search For and click Events. The Search For Events page opens.
2. Select the Software Vulnerability Detected event summary and click the Search button. The Event Search Results page opens.

Field	**Description/Action**
Check Boxes	You can use the left-side check boxes to delete events from the NA database. Once you have selected the events, click the Actions drop-down menu and click Delete. This deletes the selected events from the NA database. The adjacent Select drop-down menu enables you to select or deselect all of the events.
Date	Displays the date/time of the event in the format MMM-dd-yy HH:mm:ss. (The format is configurable by the System Administrator.)
Summary	Displays Software Vulnerability Detected. If you click the link, the Event Detail page opens, where you can view information on the security vulnerability, including: • Date • Added by • Summary • Description, including the name, Importance, and CVE (Common Vulnerabilities and Exposures) • Actions — Provides links to NA reports and external links to advisory and solution information. • Device
Host Name	Displays the host name or IP address of the device. Clicking the Host Name or IP Address opens the Device Details page, where you can view information about the device and its configuration history.
Added by	Displays the username of the person who added the event.

Summary Reports

Summary reports provide an overview of configuration activity on your network. They can help you analyze trends and identify problem areas that require particular attention. You can easily provide these reports to upper management to help communicate what your team does and the value it contributes to the organization. Because the data is presented in a standard Microsoft Excel spreadsheet, it is easy to sort and filter information and cut & paste it into other applications.

By default, NA is configured to update Summary reports on a weekly basis. Each time they are updated, the prior Summary reports file is backed up, so you can maintain an archive of these reports for historical analysis or to provide an audit trail. Reports are stored by default in *.\<install directory>\addins*.

To update the Summary reports manually:

1. On the menu bar under Tasks, click New Tasks and select Generate Summary Reports. The New Task - Generate Summary Reports page opens.
2. Make sure Start As Soon As Possible is selected.
3. Click Save Task.

The task updates the Summary reports, showing you the status of the task on the Task Information page. When the status is Succeeded, you can open the latest Summary reports.

Note: The Summary reports are available in Microsoft Excel. Excel macros are used to calculate the report data. Depending on your browser and Excel security settings, you may be prompted to enable macros when you open the Summary reports.

To open the Summary reports, on the menu bar under Reports click Summary Reports. If Summary Reports does not appear on the drop-down menu, the System Administrator should check your Administrative setting.

To navigate to specific Summary reports, you can either click the contents links on the top-level Summary report and use the Home link to return to the top-level Summary report, or use the tabs at the bottom of each report. If you do not see all the tabs at the bottom, try maximizing the window or click and drag the column adjustor to the right.

Summary Reports Descriptions

Report	Reported Information
Summary	Displays an overview of the rate of recent change activity, the most active users, and the network profile. Reports include: • Top 5 Vendors — Displays the number of devices per the top five vendors. • Top 5 OS Versions — Displays the top five OS versions that are in use. • Number of Configuration Change - Last 7 Days — Displays the average number of configuration changes per day for the past 7 days. • Change History by Time of Day — Displays when configuration changes were made. • Top 10 Most Accessed Devices — Displays the top 10 most accessed devices during the reporting period.
Change Frequency	Displays an overview of changes made in your network. The report provides the average number of changes per week over the past 30 days, broken down by users and device groups. This helps you identify top performers, as well as network areas showing a disproportionate rate of change.
Changes Per Day	Displays the number of configuration changes per day for the past two weeks. The report includes both a bar chart and table with the same data. The vertical axis shows the number of changes. The horizontal axis shows each day in the two week period.
Statistical Charts	Displays configuration changes over the past week. The Change Detection Methods pie chart shows you how changes were detected, including: • Syslog • Telnet/SSH • Proxy • Regular or manual polling • AAA • Configuration or script deployment The Change History by Time of Day bar chart shows you at what time NA detected changes. You can use these charts to monitor your changes. You can also set a policy to have network engineers make changes using the Telnet/SSH Proxy, Command Scripts, or Configuration Edit & Deploy.
Configuration Changes	Displays the following for the past week: • Change detection, including the trigger and number of changes. • Change history by time of day. • Device configuration changes, including the Host Name, IP Address, the date and time of the last change, and the User Name from Proxy, AAA, Syslog, and so on.

Report	Reported Information
Device Status	Displays the inactive devices tracked by NA. • The Top 10 Most Accessed Devices — Displays which devices took the most configuration snapshots of in the past week. Typically, these are the devices engineers are logging into or changing most often. • Device Password Changes — Displays a record of all devices whose passwords were changed in the past week. • Devices With Access Failures — Displays which devices NA could not access, either because the device was unavailable or its password information was incorrect. This list serves as a checklist to ensure NA is managing devices successfully.
Device Inventory	Displays all devices tracked by NA, including: • Host Name (from the Device Information page) • IP Address (from the Device Information page) • Asset Tag (from the Device Information page) • Location (from the configuration file) • Vendor (from the configuration file) • Model (from the configuration file) • Operating System Version (from the configuration file) • Serial Number (from the configuration file) • Device Description (from the Device Information page) • Last Snapshot Result (from tasks) • Last Modified Configuration (from tasks)
Operating System (OS) Inventory	Displays all the device OS versions running in your network, and lists how many devices are running each version. This report helps you to: • Ensure compliance with corporate standards for accepted OS versions. • Test or evaluate proposed changes to your architecture or services. • Save time when applying a vendor's security alert or patch to specific OS versions.
System Status	Displays the activity and health of the NA system. The report lists devices that do not have a device driver assigned and cannot be managed. It also provides summary information about recent system activity and the number of records in the NA database. • System Status — For devices and groups, the report displays the total number of configurations, devices, device groups, unmanaged devices, and authentication rules. For users, the report displays the total number of users and AAA users without NA accounts. The report also displays the number of custom reports. • System Activity — For tasks and messages, the report displays the total number of successful tasks, failed tasks, and system events. For the integrated Telnet/SSH client, the report displays the total number of Telnet and SSH sessions recorded. • Devices with No Driver — Displays the Host Name and IP Address of devices without drivers.

Report	Reported Information
Policy Compliance	Displays the number of policies that are and are not in compliance. The Host Name, IP Address, and the last configuration change information is displayed. The report includes both a simple pie chart with numeric totals and three tables with detailed data, including: • Configuration Policies in Compliance • Configuration Policies not in Compliance • Configuration Polices (including that name of the configuration policy and the number of associated rules).

Emailing Reports

You can email reports. On the menu bar under Reports, select New Reporting Tasks and click Email Report. The Email Report Task page opens. Refer to "Email Report Task Page Fields" on page 379 for information.

Chapter 17: Using SecurID

Use the following table to quickly locate information.

Topic	Refer to:
Getting Started	"Getting Started" on page 632
Installation Prerequisites	"Installation Prerequisites" on page 633
RSA Server Authentication Manager	"RSA Server Authentication Manager" on page 633
User Authentication	"User Autentication" on page 633
Accessing Network Devices	"Accessing Network Devices" on page 634
Adding SecurID Tokens	"Adding SecurID Software Tokens" on page 636
Logging Into NA Using SecurID	"Logging In Using SecurID" on page 637
SecurID Troubleshooting	"SecurID Troubleshooting" on page 639

Getting Started

The RSA SecurID solution is designed to protect your organization by helping to ensure that only authorized users are granted access to networked resources. In general, SecurID is a two part authentication scheme, requiring a password/PIN, along with a physical hardware component. The hardware component changes its passcode every 60 seconds. Some device makers incorporate this authentication system into their network devices. Please refer to your SecurID documentation for detailed information on how SecurID works.

Note: When NA is configured to use SecurID for external authentication, Single Sign-on functionality will not be enabled when connecting to the NA proxy. You will need to authenticate again using your SecurID credentials because SecurID passcodes cannot be reused.

HP Network Automation (NA) supports SecurID for highly secure, two-factor authentication for:

- Authenticating users logging into NA
- Accessing network devices through NA

The following table describes NA SecurID support.

Accessing NA	Connection Method	SecurID Support
Web User Interface	HTTP	Yes
SSH/Telnet Proxy	SSH Telnet	Yes Yes
API	RMI	No

Note: To use SSH with SecurID authentication with a device, you must first ensure that the device supports SecurID over SSH using keyboard interactive, and specifically supports Next-token-code mode.

Installation Prerequisites

When using SecurID to login to NA, NA supports the following token algorithms and token versions:

- AES SDTID 3.0
- SID SDTID 2.0

Note: RSA SecurID 6.1 does not work when NA is installed on a Windows 2k3 (64-bit) platform.

RSA Server Authentication Manager

During installation, the NA Installer installs the *rsa_api.properties* file in the NA_DIRECTORY/jre directory. You must edit this file to include:

- RSA_AGENT_HOST — The IP Address of the server on which NA resides.
- SDCONF_LOC — The location of the RSA conf file that is generated by the RSA Server Authentication Manager.

The example below shows that NA is installed on a server with the IP Address of 10.255.140.124. The RSA conf file is located in c:\NA\jre\sdconf.rec.

```
RSA_AGENT_HOST=10.255.140.124
SDCONF_LOC=C:/NA/jre/sdconf.rec (Unix platform)
SDCONF_LOC=C:\\NA\\jre\\sdconf.rec (Windows platform)
```

User Autentication

For user authentication into NA, make sure:

- You have purchased hardware or software tokens from RSA.
- The ACEServer is running and accessible from the NA server.
- On the ACEServer, the host where NA is running is added as an Agent Host.
- In the Agent Host settings, the Agent type is “UNIX Agent.”
- You created users on the ACEServer.
- You assigned software tokens to the ACEServer users.
- You enabled users to connect from Agent Hosts.

For NA to access devices, make sure:

- NA is running.
- The RSA software token software is installed on the NA server.
- The ACEServer is running and accessible from the devices.
- You have obtained software tokens from RSA.
- You have imported the SecurID tokens to the NA server using the RSA Software Token application.
- You have added licenses to the ACEServer.

- You have created a user on the ACEServer.
- You have assigned a software token to the user.
- You have set the PIN for the token.
- You have enabled the user to connect to the devices.
- In NA, you added a user corresponding to the SecurID user.
- You selected if you are using unique per user tokens or a pool of tokens.
- You assigned a token pool username if using a token pool.
- You assigned the token to the user.

Accessing Network Devices

For access from NA to devices, you will need to download software token software and licenses from RSA. Hardware token licenses, such as FOBS and pinpads, cannot be used.

You can download the software token software from RSA's Website. Be sure to install the software on the same system on which NA is installed. You will also need to import the software token licenses to this system through the normal SecurID mechanisms.

Note: The ACEServer and the server running NA need to be time synchronized. Evidently, software tokens are sensitive to time differences. If the two servers are more than a minute out of sync, the generated passcodes could fail. You can use NTP on both servers to keep the clocks accurate.

NA monitors access to devices when using SecurID to ensure that a given tokencode is not used twice. This means that activities in NA might be slower when using SecurID device access. To address this, NA provides the ability to load multiple software token seeds into the system. You can use one of the following token management modes:

- Per user — Each NA user has one or more corresponding software token seeds. In this mode, each device access uses only the seed(s) corresponding to the user that initiated the task or NA proxy connection. It is recommended that all users in the system have valid software tokens assigned.
  - On the Home page under My Settings, click My Profile. The My Profile page opens. Refer to “My Profile Page Fields” on page 262 for information on the My Profile page fields.

  Note: Refer to “Adding SecurID Software Tokens” on page 636 for information on adding and/or updating SecurID tokens.

- Pool — A pool of general use software token seeds are provided to NA and used as efficiently as possible for maximum performance. On the menu bar under Admin, select Administrative Settings and click the Device Access option. The Device Access page opens, where you can configure SecurID device access. Refer to “Device Access Page Fields” on page 47 for information.

Once software seeds have been loaded into NA, you can designate specific devices or sets of devices for management via RSA SecurID authentication. To enable SecurID access to a specific device:

1. On the menu bar under Devices, click Inventory. A list of all managed devices opens.
2. Click the device for which you want to enable SecurID access. The Device Details page opens.
3. In the Action column, click Edit. The Edit Device page opens. Refer to "New Device Page Fields" on page 108 for information.
4. Scroll down to the Password Information section and select the Use device-specific password information option.
5. Scroll down and click the Show Device Access Settings (device-specific settings) field.
6. Select "Use SecurID" from the Setting drop-down menu and enter either *exec* or *enable* for the Value. If you want to use SecurID in Exec Mode, enter *exec*. Using *exec* enables Exec Mode, typically the first mode you are in when logging into a device. If you want to use SecurID in both Exec Mode and Enable Mode, enter *enable*.
7. If you want this device to use a specific user pool of SecurID tokens, in the Custom Setting field, enter: *securid_pool_override*. In the Value field, enter the username.
8. Click the Save Device button.

When a device (or group of devices) is configured for SecurID access and software seeds have been entered, NA automatically generates the correct time-limited tokencode each time it needs to access the device.

You can also setup a network password rule on devices for management via RSA SecurID authentication. Refer to "Device Password Rule Page Fields" on page 136 for information. Then follow Steps 4, 5, and 6 above.

Adding SecurID Software Tokens

To add SecurID software tokens:

1. Using the RSA Software Token application, import the tokens to the server where NA is running.
2. On the Home page under My Settings, click My Profile. The My Profile page opens. Refer to "My Profile Page Fields" on page 262 for information on the My Profile page fields.
3. Under the SecurID section at the bottom of the page, click the Manage Software Token licenses link. The View SecurID Tokens page opens, where you can view, add, and/or update software token licenses associated with your user login. These licenses are used to login into devices if the devices are configured to require SecurID credentials.
4. Click the Add Token link. The New SecurID Tokens page opens. You can add a single software token or a pool of general use software tokens per user.

Note: You can also navigate to the Manage Software Token licences link by clicking the Users option under Administration and then clicking the Edit option for that user.

New SecurID Tokens Page

Field	Description/Action
SecurID User	Enter the username assigned to the token on the ACEServer.
Software Token Serial Number	Enter the serial number of the token (zero padded).
PIN	If a PIN is configured for the token when issued from the ACE/Server, enter it here. (**Note**: If the PIN is updated, it must also be updated here.)
Confirm PIN	Re-enter the PIN for confirmation.
Password	If a password is configured for the token when issued from the ACE/Server enter it here.

Be sure to click Save when you are done.

Logging In Using SecurID

You can designate RSA SecurID as the external authentication mechanism. Refer to "User Authentication Page Fields" on page 79 for information.

You must install the *sdconf.rec* file from the RSA SecurID ACE server onto the NA server (for example: *C:\WINDOWS\SYSTEM32\sdconf.rec)*. This file provides the necessary connection information for NA to access SecurID.

Note: On a Linux or Solaris platform, by default NA looks for the *sdconf.rec* file in the */var/ace* directory. This file provides the necessary connection information for NA to access SecurID.

Upon completing the install, it is necessary to restart the NA Management Engine. Refer to "Starting and Stopping Services" on page 96 for information on restarting the NA Management Engine.

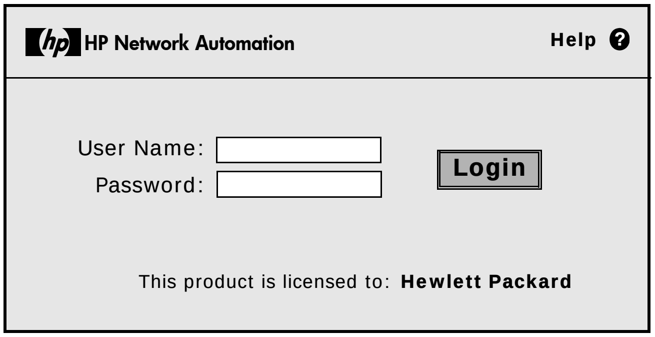
There are two methods for logging into NA via SecurID if the token is in New Pin mode:

- Using a SecurID system PIN
- Using a new SecurID PIN

In all cases, RSA's login procedures require users to re-authenticate with the new PIN.

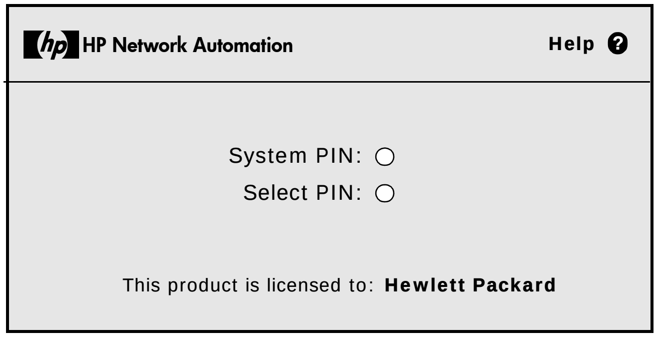
At the NA login prompt (as shown below):

1. Enter your NA username.
2. Enter your passcode in the Password field.
3. Click Login.



This product is licensed to: **Hewlett Packard**

If your SecurID system is configured to prompt you to use either a System PIN or a new PIN, the following page opens.



This product is licensed to: **Hewlett Packard**

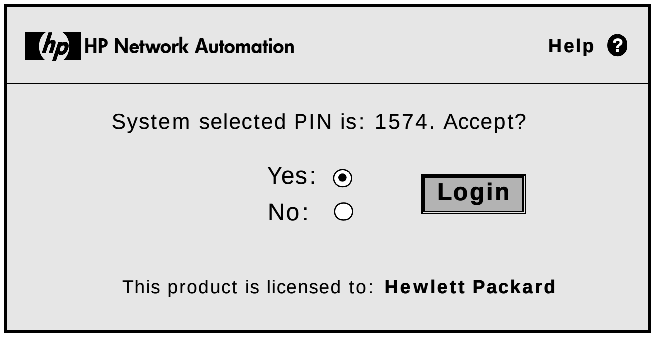
If you click System PIN, refer to "Login Method One: Using a System PIN" on page 638. If you click Select PIN, refer to "Login Method Two: Using a New PIN" on page 638.

Note: If your SecurID system is not configured to prompt you for either a System PIN or a new PIN, refer to either Login Method One or Login Method Two depending on your SecurID system configuration.

Login Method One: Using a System PIN

At the login page:

1. Click System PIN, as shown on page 460. After you have attained a System PIN from SecurID, click Yes, as shown below.
2. Click Login.
3. You are prompted to wait and use the next tokencode to login.



System selected PIN is: 1574. Accept?

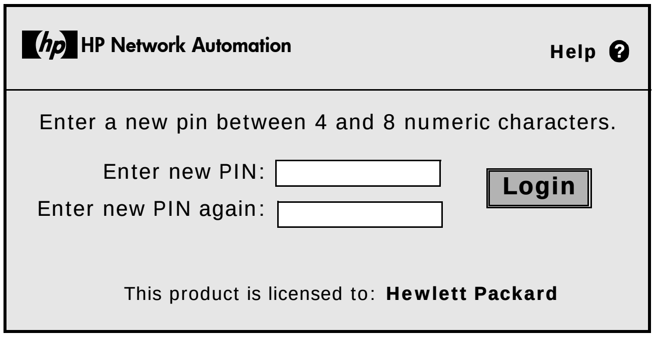
Yes: ●
No: ○

This product is licensed to: **Hewlett Packard**

Login Method Two: Using a New PIN

At the login page:

1. Click Select PIN, as shown on page 402.
2. Enter the new PIN twice, as shown below.
3. Click Login. The PIN is checked for adherence to the PIN parameters.



Enter a new pin between 4 and 8 numeric characters.

Enter new PIN:
Enter new PIN again:

This product is licensed to: **Hewlett Packard**

SecurID Troubleshooting

I. If you cannot login to NA using SecurID, contact your RSA Administrator.

II. If you are using SecurID for device access, it is recommended that you turn off the Syslog User Identification option for change detection, or you could receive Snapshot Task Failed messages.

1. On the menu bar under Admin, select click Administrative Settings and click Configuration Mgmt. The Configuration Mgmt page opens.
2. At the Change User Identification section — Syslog User Identification, uncheck the “Identify who made a configuration change from the syslog message text, if possible.” check box.
3. At the Change User Identification section — Auto-Create Users from Syslog, uncheck the “Create new users in NA when the change author identified from syslog does not already exist (Auto-Create Users must be enabled).” check box.
4. Click the Save button.

III. If external authentication fails, NA attempts to fall-back to the local user credentials in the following cases:

- When the external authentication service is down or inaccessible.
- For static user accounts that have never successfully logged in via an external authentication method.
- For the built-in Admin user account.

IV. The Node Secret file is used to authenticate communication between the RSA ACE/Agent client and RSA ACE/Server. If you see the following type of message in the ACE/Server log file, you must update the Node Secret file for the NA server.

```
07/12/2006 22:00:19U ----/core15.hp.com        ---->/
07/12/2006 18:00:19L Node verification failed      NArsa.rduNA.HP.com
```

To create a Node Secret:

1. Click Agent Host --> Add (or Edit) Agent Host.
2. Click Create Node Secret.
3. In the Password box, enter a password and then enter it again in the Confirm Password box.
4. If you want to save the Node Secret file under the default name and directory, click OK. The Node Secret file is created in the default directory using the default name *nodesecret.rec*. The default directory is *ACEPROG* until you specify a different directory, in which case the directory you specify becomes the default directory until you restart the Database Administration application. If you want to save the file under a different name, click Browse. In the Node Secret Filename Specification dialog box, change the name and directory, and then click Save.

   Note: If a Node Secret file with the same name exists in the specified directory, click

Yes to overwrite it or click No to return to the Node Secret Filename Specification dialog box. When you click Yes, the Node Secret file is created using the name and directory you specify.

In the Add (or Edit) Agent Host dialog box, the Create Node Secret File button is unavailable. Node Secret Created is selected.

5. Click OK.
6. Copy the new Node Secret file to the Agent host.
7. Copy the Load Node Secret utility (*agent_nsload*) from the RSA Authentication Manager media to the Agent host. Be sure to copy the correct *agent_nsload* process for the operating system of the Agent host.
8. On the Agent host, run the Load Node Secret utility to load the new Node Secret file. On the command line prompt, enter: `agent_nsload –f path –p password` (where `path` is the directory location and name of the Node Secret file and `password` is the password used to protect the Node Secret file.)

   Note: If your ACE/Server is on a different platform than your NA server, the *agent_nsload* executable might not be compatible. In this case, please contact RSA to get the correct binary. In addition, you might have to reboot the NA server so that RSA dlls can locate the new Node Secret file.

Chapter 18: Compliance Center

Use the following table to quickly locate information.

Topic	Refer to:
Getting Started	"Getting Started" on page 642
COBIT Compliance Status reports	"COBIT Compliance Status Reports" on page 644
COSO Compliance Status reports	"COSO Compliance Status Reports" on page 652
ITIL Compliance Status reports	"ITIL Compliance Status Reports" on page 655
GLBA Compliance Status reports	"GLBA Compliance Status Reports" on page 658
HIPAA Compliance Status reports	"HIPAA Compliance Status Reports" on page 661
PCI Data Security Standard Compliance Status reports	"PCI Data Security Standard Compliance Status Reports" on page 668

Note: HP Compliance Center is based on HP's understanding of the regulations and standards presented. HP is not an auditor or legal authority, and you should consult your corporate auditor or legal representative for guidance.

Getting Started

The Compliance Center is NA’s portal for accessing reports and information that help determine the current compliance status of your network infrastructure with respect to Sarbanes-Oxley (Section 404) and supporting internal control frameworks.

The Public Company Accounting Reform and Investor Protection Act of 2002, commonly known as Sarbanes-Oxley, is designed to improve the accuracy and reliability of corporate disclosures to investors. Sarbanes-Oxley generally applies to all U.S. companies registered with or required to file reports with the SEC (Securities and Exchange Commission). The regulation requires the CEO and CFO of reporting companies to certify their companies’ SEC reports.

A key provision of Sarbanes-Oxley is Section 404, which specifically addresses internal control over financial reporting. Section 404 requires that reporting companies include an internal control report and assessment as part of their financial reporting. Sarbanes-Oxley (Section 404) provides no specific control requirements for IT-related compliance efforts, so organizations must select an internal control framework, such as COSO, COBIT, ITIL, or PCI Data Security Standard and enforce and report against that framework. For detailed information regarding Sarbanes-Oxley (Section 404) compliance using NA, refer to the online information presented on the Compliance Center Home page.

To access the Compliance Center Home page, on the menu bar under Reports, click Compliance Center. The Compliance Center Home page opens.

Compliance Center Home Page

Options	Description/Action
Sarbanes-Oxley (Section 404)	Opens the Sarbanes-Oxley (Section 404) Compliance Status overview information.
COBIT Compliance Status link	Opens the COBIT Compliance Status report. Refer to "COBIT Compliance Status Reports" on page 644 for information.
COSO Compliance Status link	Opens the COSO Compliance Status report. Refer to "COSO Compliance Status Reports" on page 652 for information.
ITIL Compliance Status link	Opens the ITIL Compliance Status report. Refer to "ITIL Compliance Status Reports" on page 655 for information.
GLBA Compliance Status link	Opens the GLBA Compliance Status report. Refer to "GLBA Compliance Status Reports" on page 658 for information.
HIPAA Compliance Status link	Opens the HIPAA Compliance Status report. Refer to "HIPAA Compliance Status Reports" on page 661 for information.
PCI Data Security Standard Compliance Status link	Opens the PCI Data Security Standard report. Refer to "PCI Data Security Standard Compliance Status Reports" on page 668 for information.

COBIT Compliance Status Reports

COBIT (Control Objectives for Information and related Technology) is an internal control framework that helps meet the needs of management by bridging the gaps among business risks, control needs, and technical issues, while balancing risk versus return over IT and its processes.

NA enhances the implementation of four domains for effective internal control system as defined by COBIT:

- Monitoring — NA monitors processes, assesses internal control adequacy, secures independent assurance, and provides for independent audit.
- Delivery & Support — NA helps to manage service levels, third-party services, and performance and capacity, ensure continuous service system security, identify and allocate costs, educate and train users, assist and advise customers, and manage configurations, data, facilities, and operations.
- Planning & Organization — NA helps to define a strategic IT plan, determine technological direction, manage the IT investment and human resources, communicate management aims and directions, and ensure compliance with external requirements.
- Acquisition & Implementation — NA helps to identify automated solutions, acquire and maintain technology infrastructure, develop and maintain procedures, install and accredit systems, and manage changes.

For detailed information on COBIT and how NA enhances the implementation of COBIT, click the “More information about COBIT and achieving compliance using HP Network Automation” link on the COBIT Status Compliance page.

To view the COBIT Compliance Status reports:

1. On the menu bar under Reports, click Compliance Center. The Compliance Center Home page opens.
2. Click the COBIT Compliance Status link. The COBIT Compliance Status page opens.

COBIT Compliance Status Page Fields

Fields	Description/Action
MONITORING	
M1 Monitor the processes	Displays the number of: • Devices with different startup and running configurations. Clicking the Device List link opens Device Search Results report. • Inactive devices. Clicking the Inactive Devices link opens the Device Search Results page. • ACLs. Clicking the All ACLs link opens the ACLs Search Results page. • ACLs in use. Clicking the ACLs In Use link opens the ACLs Search Results page. • ACL changes in the last 7 days. Clicking the ACL Changes link opens the ACLs Search Results page. • Approved changes in the last 7 days. Clicking the Approved Changes link opens the Approved Changes Search Results page.
M2 Assess internal control adequacy	Displays the number of: • Workflow rules in place. Clicking the Workflow Setup link opens the Workflow Wizard. • Configuration polices in place. Clicking the Configuration Polices link opens the Polices page. • Unapproved changes in the last 7 days. Clicking the Unapproved Changes link opens the Unapproved Changes Search Results page.
M3 Obtain independent assurance	Displays the number of: • Monitors showing an “okay” status. Clicking the System Status link opens the System Status report. • Devices in software level. Clicking the Device Software Report link opens the Software Level Search Results page. • Configuration policy non-compliance events in the last 24 hours. Clicking the Configuration Policy Events (24 hours) link opens the Configure Policy Activity page. • Configuration policy non-compliance events in the last 7 days. Clicking the Configuration Policy Events (7 days) link opens the Configure Policy Activity page. • Configuration management “Best Practices” green (within threshold) statuses. Clicking the Network Status Report link opens the Network Status report.
M4 Provide for independent audit	Displays the number of: • Accessible User reports. Clicking the User & System Reports link opens the User & System Reports page. • Accessible System reports. Clicking the User & System Reports link opens the User & System reports.

Fields	Description/Action
DELIVERY & SUPPORT	
DS1 Define and manage service levels	Displays the number of: • Configuration management "Best Practices" green (within threshold) statuses. Clicking the Network Status Report link opens the Network Status report. • Average changes per day (last 7 Days). Clicking the Summary Reports link opens the Summary reports. • Average changes per day (last 30 Days). Clicking the Summary Reports link opens the Summary reports.
DS2 Manage third-party services	Displays the number of: • Devices with access failures. Clicking the Inaccessible Devices link opens the Device Search Results page. • Devices that have different startup and running configurations. Clicking the Devices List link opens the Device Search Results page. • Inactive devices. Clicking the Inactive Devices link opens the Device Search Results page.
DS3 Manage performance and capacity	Displays the number of devices with port availability less than 10%. Clicking the Port Availability link opens the Device Search Results page.
DS4 Ensure continuous service	Displays the number of: • Diagnostics run in the last 24 hours. Clicking the Diagnostics (24 hours) link opens the Diagnostic Search Results page. • Diagnostics run in the last 7 days. Clicking the Diagnostics (7 days) link opens the Diagnostic Search Results page.
DS5 Ensure systems security	Displays the number of: • Users restricted to specific sets of devices. Clicking the User List link opens the User Search Results page. • Users assigned Administrator access permissions. Clicking the User List link opens the All User page. • Device Password Rules in place. Clicking the Device Password Rules link opens the Device Password Rules List page. • ACLs. Clicking the All ACLs link opens the ACLs Search Results page. • ACLs in use. Clicking the ACLs In Use link opens the ACLs Search Results page. • ACL changes in the last 7 days. Clicking the ACL Changes link opens the ACLs Search Results page.
DS6 Identify and allocate costs	Displays the number of: • Devices in inventory. Clicking the Device List link opens the Inventory page. • Modules in inventory. Clicking the Module link opens the Module Search Results page.

Fields	Description/Action
DS7 Educate and train users	Provides links to the following documentation: • *NA User Guide* • *NA Release Notes*
DS8 Assist and advice customers	Provides links to the following: • Download driver update packages • View latest Release Notes • View license Information • Create a Technical Support ticket • Email Customer Support
DS9 Manage the configuration	Displays the number of: • Configuration changes detected in the last 7 days. Clicking the Configuration Changes link opens the Config Search Results page. • Stored device configurations. Clicking the Active Configurations link opens the Config Search Results page. • Changes pending approval. Clicking the Changes Pending Approval link opens the Changes Pending Search Results page. • Approved changes in the last 7 days. Clicking the Approved Changes link opens the Approved Changes Search Results page. • Unapproved changes in the last 7 days. Clicking the Unapproved Changes link opens the Unapproved Changes Search Results page.
DS10 Manage problems and incidents	Displays the number of: • Configuration Changes detected in the last 24 hours. Clicking the Dashboard link opens the Home page. • NA events that occurred in the last 24 hours. Clicking the Dashboard link opens the Home page.
DS11 Manage data	Displays the number of stored device configurations.
DS12 Manage facilities	Displays the number of: • Devices in inventory. Clicking the Device List link opens the Inventory page. • Modules in inventory. Clicking the Modules link opens the Module Search Results page.

Fields	Description/Action
DS13 Manage operations	Displays the number of: • Device change tasks scheduled for the next 24 hours. Clicking the Pending Tasks (24 hours) link opens the Task Search Results page. • Device change tasks scheduled for the next 7 days. Clicking the Pending Tasks (7 days) link opens the Task Search Results page. • Software deployments scheduled for the next 24 hours. Clicking the Pending Deployments (24 hours) link opens the Task Search Results page. • Software deployments scheduled for the next 7 days. Clicking the Pending Deployments (7 days) link opens the Task Search Results page. • Changes pending approval. Clicking the Changes Pending Approval link opens the Changes Pending Search Results page.
PLANNING & ORGANIZATION	
PO1 Define a strategic IP plan	Displays the number of: • Devices in inventory. Clicking the Device List link opens the Device Details page. • Modules in inventory. Clicking the Modules link opens the Module Search Results page. • Displays the number of devices with port availability less than 10%. Clicking the Port Availability link opens the Device Search Results page.
PO2 Define the information architecture	Displays the number of: • Devices in inventory. Clicking the Device List link opens the Inventory page. • Modules in inventory. Clicking the Modules link opens the Module Search Results page. • Stored device configurations. Clicking the Active Configurations link opens the Config Search Results page.
PO3 Determine the technological direction	Displays the number of devices in inventory from the total number of vendors. Clicking the Device List by Vendors link opens the Inventory page.
PO4 Define the IT organization and relationships	Displays the number of: • Users restricted to specific sets of devices. Clicking the User List link opens All Users page. • Users assigned Administrator access permissions Clicking the User List link opens the All Users page. • Device Password Rules in place Clicking the Device Password Rules link opens the Device Password Rules List page
PO5 Manage the IT investment	Displays the number of: • Devices in inventory. Clicking the Device List link opens the Inventory page. • Modules in inventory. Clicking the Modules link opens the Module Search Results page. • Devices not active. Clicking the Device List link opens the Inventory page.

Fields	Description/Action
PO6 Communicate management aims and directions	Displays the number of: • Configuration management “Best Practices” green (within threshold) statuses. Clicking the Network Status Report link opens the Network Status report. • Active configurations policies. Clicking the Configurations Policies link opens the Config Search Results page.
PO7 Manage human resources	Displays the number of: • Users restricted to specific sets of devices. Clicking the User List link opens the User Search Results page. • Users assigned Administrator access permissions. Clicking the User List link opens the User Search Results page. • Device Password Rules in place. Clicking the Device Password Rules link opens the Device Password Rules List page.
PO8 Manage compliance with external requirements	Displays the number of active configurations policies. Clicking the Configurations Policies link opens the Config Search Results page. Clicking the Compliance Center link opens the Compliance Center Home page.
PO9 Assess risks	Displays the number of: • Configuration management “Best Practices” green (within threshold) statuses. Clicking the Network Status Report link opens the Network Status report. • Devices with access failures. Clicking the Inaccessible Devices link opens the Device Search Results page. • Displays the number of devices with port availability less than 10%. Clicking the Port Availability link opens the Device Search Results page.
PO10 Manage projects	Displays the number of: • Device change tasks scheduled for the next 24 hours. Clicking the Pending Tasks (24 hours) link opens the Task Search Results page. • Device change tasks scheduled for the next 7 days. Clicking the Pending Tasks (7 days) link opens the Task Search Results page. • Software deployments scheduled for the next 24 hours. Clicking the Pending Deployments (24 hours) link opens the Task Search Results page. • Software deployments scheduled for the next 7 days. Clicking the Pending Deployments (7 days) link opens the Task Search Results page.
PO11 Manage quality	Displays the number of: • Monitors showing an “okay” status. Clicking the System Status link opens the System Status report. • Devices in software compliance. Clicking the Device Software Report link opens the Software Compliances Search Results page. • Configuration policy non-compliance events in the last 24 hours. Clicking the Policy Events (24 hours) link opens the Configure Policy Activity page. • Configuration policy non-compliance events in the last 7 days. Clicking the Policy Events (7 days) link opens the Configure Policy Activity page. • Configuration management “Best Practices” green (within threshold) statuses. Clicking the Network Status Report link opens the Network Status report.

Fields	Description/Action
ACQUISTION & IMPLEMENTATION	
AI1 Identify automated solutions	Provides the following default links: • System task to prune database runs weekly. Clicking the Pending Tasks link opens the Pending Tasks page. • System task to gather module inventory data runs weekly. Clicking the Pending Tasks link opens the Scheduled Tasks page. • System task to update Summary Reports runs daily. Clicking the Pending Tasks link opens the Scheduled Tasks page. • System task to poll for device configuration changes runs daily. Clicking the Pending Tasks link opens the Scheduled Tasks page.
AI2 Acquire and maintain application software	This is not applicable.
AI3 Acquire and maintain technology infrastructure	Displays the number of: • Devices in inventory. Clicking the Device List link opens the Inventory page. • Modules in inventory. Clicking the Modules link opens the Module Search Results page. • Stored device configurations. Clicking the Active Configurations link opens the Config Search Results page.
AI4 Develop and maintain procedures	Displays the number of: • Configuration management “Best Practices” green (within threshold) statuses. Clicking the Network Status Report link opens the Network Status report. • Active configurations policies. Clicking the Configurations Policies link opens the Config Search Results page.
AI5 Install and accredit systems	Displays the number of: • Monitors showing an “okay” status. Clicking the System Status link opens the System Status report. • Device software compliance. Clicking the Device Software Report link opens the Software Levels Search Results page. • Configuration management “Best Practices” green (within threshold) statuses. Clicking the Network Status Report link opens the Network Status report.

Fields	Description/Action
AI6 Manage changes	Displays the number of: • Telnet/SSH Proxy sessions in the last 7 days. Clicking the Sessions link opens the Session Search Results page. • Device change tasks scheduled in the last 7 days. Clicking the Past Tasks (7 days) link opens the Task Search Results page. • Device change tasks scheduled for the next 7 days. Clicking the Pending Tasks (7 days) link opens the Task Search Results page.. • Changes pending approval. Clicking the Changes Pending Approval link opens Changes Pending Search Results page. • Approved changes in the last 7 days. Clicking the Approved Changes link opens the Approved Changes Search Results page. • Unapproved changes in the last 7 days. Clicking the Unapproved Changes link opens the Unapproved Changes Search Results page.

COSO Compliance Status Reports

In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued a landmark report on internal control. *Internal Control—Integrated Framework*, which is often referred to as “COSO”, provides a basis for establishing internal control systems and determining their effectiveness.

NA provides five essential components for an effective internal control system:

- Control Environment — Establishes the foundation for the internal control system by providing fundamental discipline and structure.
- Risk Assessment — Includes identification and analysis by management of relevant risks to achieving objectives.
- Control Activities — Ensures management objectives are achieved and risk mitigation strategies are carried out.
- Information and Communication — Supports all control components by communicating control responsibilities to employees, and by providing information in a form and timeframe that enables employees to carry out their duties.
- Monitoring — Includes the external oversight of internal controls by management or other parties outside the process.

For detailed information on COSO, click the “More information about COSO and achieving compliance using HP Network Automation” link.

To view the COSO Compliance Status reports:

1. On the menu bar under Reports, click Compliance Center. The Compliance Center Home page opens.
2. Click the COSO Compliance Status link. The COSO Compliance Status page opens.

COSO Compliance Status Page Fields

Fields	**Description/Action**
Control Environment	Displays the number of: • Users restricted to specific sets of devices. Clicking the User List link opens the User Search Results page. • Users assigned Administrator access permissions Clicking the User List link opens the User Search Results page. • Device Password Rules in place. Clicking the Device Password Rules link opens the Device Password Rules List page. • Configuration polices in place. Clicking the Configuration Polices link opens the Polices page. • Workflow rules in place. Clicking the Workflow Setup link opens the Workflow Wizard. • ACLs. Clicking the All ACLs link opens the ACLs Search Results page. • ACLs in use. Clicking the ACLs In Use link opens the ACLs Search Results page.

Fields	Description/Action
Risk Assessment	Displays the number of: • Configuration management "Best Practices" green (within threshold) statuses. Clicking the Network Status Report link opens the Network Status report. • Devices with access failures. Clicking the Inaccessible Devices link opens the Device Search Results page. • Displays the number of devices with port availability less than 10%. Clicking the Port Availability link opens the Device Search Results page.
Control Activities	Displays the number of: • Telnet/SSH Proxy sessions in the last 7 days. Clicking the Sessions link opens the Session Search Results page. • Device change tasks scheduled for the next 24 hours. Clicking the Pending Tasks (24 hours) link opens the Task Search Results page. • Device change tasks scheduled for the next 7 days. Clicking the Pending Tasks (7 days) link opens the Task Search Results page. • Software deployments scheduled for the next 24 hours. Clicking the Pending Deployments (24 hours) link opens the Task Search Results page. • Software deployments scheduled for the next 7 days. Clicking the Pending Deployments (7 days) link opens the Task Search Results page. • Changes pending approval. Clicking the Changes Pending Approval link opens Changes Pending Search Results page.
Information and Communication	Displays the number of: • Configuration changes detected in the last 24 hours. Clicking the Dashboard link opens the Home page. • NA events that occurred in the last 24 hours. Clicking the Dashboard link opens the Home page. • Average number of changes per day (last 7 days). Clicking the Summary Reports link opens the Summary reports. • Average number of changes per day (last 30 days). Clicking the Summary Reports link opens the Summary reports.

Fields	Description/Action
Monitoring	Displays the number of: • Monitors showing an “okay” status. Clicking the System Status link opens the System Status report. • Device software compliance. Clicking the Device Software Report link opens the Software Compliance Search Results page. • Configuration policy non-compliance events in the last 24 hours. Clicking the Configuration Policy Events (24 hours) link opens the Configure Policy Activity page. • Configuration policy non-compliance events in the last 7 days. Clicking the Configuration Policy Events (7 days) link opens the Configure Policy Activity page. • Devices that have different startup and running configurations. Clicking the Devices List link opens the Device Search Results page. • Inactive devices. Clicking the Inactive Devices link opens the Device Search Results page. • Approved changes in the last 7 days. Clicking the Approved Changes link opens the Approved Changes Search Results page. • Unapproved changes in the last 7 days. Clicking the Unapproved Changes link opens the Unapproved Changes Search Results page. • ACL changes in the last 7 days. Clicking the ACL Changes link opens the ACLs Search Results page.

ITIL Compliance Status Reports

ITIL (IT Infrastructure Library) was developed for the British government by the CCTA (now the OGC: Office of Government Commerce), and has been rapidly adopted across the world as the standard for best practice in the provision of IT services. Three major areas of ITIL include:

- Service Support — Enables IT services to be effectively provided.
- Service Delivery — Enables the management of IT services.
- Security Management — Enables the protection of data and infrastructures.

For detailed information on ITIL, click the “More information about ITIL and achieving compliance using HP Network Automation” link.

To view the ITIL Compliance Status reports:

1. On the menu bar under Reports, click Compliance Center. The Compliance Center Home page opens.
2. Click the ITIL Compliance Status link. The ITIL Compliance Status page opens.

ITIL Compliance Status Page Fields

Fields	Description/Action
Configuration Management	
service support process	Displays the number of: • Configuration changes detected in the last 7 days. Clicking the Configuration Changes link opens the Config Search Results page. • Stored device configurations. Clicking the Active Configurations link opens the Config Search Results page.
Incident Management	
Service support process	Displays the number of: • Configuration changes detected in the last 24 hours. Clicking the Dashboard link opens the Home page. • NA events that occurred in the last 24 hours. Clicking the Dashboard link opens the Home page.
Problem Management	
Service support process	Displays the number of: • Configuration management “Best Practices” green (within threshold) statuses. Clicking the Network Status Report link opens the Network Status report. • Devices with access failures. Clicking the Inaccessible Devices link opens the Device Search Results page.

Fields	Description/Action
Change Management	
Service support process	Displays the number of: • Telnet/SSH Proxy sessions in the last 7 days. Clicking the Sessions link opens the Session Search Results page. • Device change tasks scheduled for the next 24 hours. Clicking the Pending Tasks (24 hours) link opens the Task Search Results page. • Device change tasks scheduled for the next 7 days. Clicking the Pending Tasks (7 days) link opens the Task Search Results page. • Changes pending approval. Clicking the Changes Pending Approval link opens Changes Pending Search Results page. • Approved changes in the last 7 days. Clicking the Approved Changes link opens the Approved Changes Search Results page. • Unapproved changes in the last 7 days. Clicking the Unapproved Changes link opens the Unapproved Changes Search Results page. • Configuration polices in place. Clicking the Configuration Polices link opens the Policies page. • Workflow rules in place. Clicking the Workflow Setup page opens the Workflow Wizard.
Service Desk	
Service support function	Displays the number of: • Device change tasks scheduled for the next 24 hours. Clicking the Pending Tasks (24 hours) link opens the Task Search Results page. • Device change tasks scheduled for the next 7 days. Clicking the Pending Tasks (7 days) link opens the Task Search Results page.
Release Management	
Service support process	Displays the number of: • Software deployments scheduled for the next 24 hours. Clicking the Pending Deployments (24 hours) link opens the Task Search Results page. • Software deployments scheduled for the next 7 days. Clicking the Pending Deployments (7 days) link opens the Task Search Results page. • Devices in software compliance. Clicking the Device Software Report link opens the Software Compliance Search Results page.
Service Level Management	
Service delivery process	Displays the number of: • Configuration management “Best Practices” green (within threshold) statuses. Clicking the Network Status Report link opens the Network Status report. • Average changes per day (last 7 Days). Clicking the Summary Reports link opens the Summary reports. • Average changes per day (last 30 Days). Clicking the Summary Reports link opens the Summary reports.

Fields	Description/Action
Capacity Management	
Service delivery process	Displays the number of devices with port availability less than 10%. Clicking the Port Availability link opens the Device Search Results page.
Continuity Management	
Service delivery process	Displays the number of: • Diagnostics run in the last 24 hours. Clicking the Diagnostics (24 hours) link opens the Diagnostic Search Results page. • Diagnostics run in the last 7 days. Clicking the Diagnostics (7 days) link opens the Diagnostic Search Results page.
Availability Management	
Service delivery process	Displays the number of: • Configuration policy non-compliance events in the last 24 hours. Clicking the Configuration Policy Events (24 hours) link opens the Configure Policy Activity page. • Configuration policy non-compliance events in the last 7 days. Clicking the Configuration Policy Events (7 days) link opens the Configure Policy Activity page.
IT Financial Management	
Service delivery process	Displays the number of: • Monitors showing an “okay” status. Clicking the System Status link opens the System Status report. • Devices in inventory. Clicking the Device List link opens the Inventory page. • Modules in inventory. Clicking the Module link opens the Module Search Results page
Security Management	
Service delivery process	Displays the number of: • Users restricted to specific sets of devices. Clicking the User List link opens the All Users page. • Users assigned Administrator access permissions. Clicking the User List link opens the User Search Results page. • Device password rules in place. Clicking the Device Password Rules link opens the Device Password Rules List page. • ACLs. Clicking the All ACLs link opens the ACLs Search Results page. • ACLs in use. Clicking the ACLs In Use link opens the ACLs Search Results page. • ACL changes in the last 7 days. Clicking the ACL Changes link opens the ACLs Search Results page.

GLBA Compliance Status Reports

The Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA), includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal privacy requirements:

- Pretexting provisions
- Financial Privacy Rule
- Safeguards Rule

The Safeguards Rule requires all financial institutions to design, implement, and maintain safeguards to protect customer information. The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions, such as credit reporting agencies that receive customer information from other financial institutions.

For detailed information on GLBA, click the "More information about GLBA and achieving compliance using HP Network Automation" link.

To view the GLBA Compliance Status reports:

1. On the menu bar under Reports, click Compliance Center. The Compliance Center Home page opens.
2. Click the GLBA Compliance Status link. The GLBA Compliance Status page opens.

GLBA Compliance Status Page Fields

Fields	Description/Action
Interagency Guideline Section	
II.A. Information Security Program	Displays the number of: • Devices in inventory. • Modules in inventory. • Stored device configurations.
II.B. Objectives	Displays the number of: • Users restricted to specific groups of devices. • Users assigned Administrator permissions. • Failed user login attempts in the past 7 days. • Changes pending approval. • Approved changes in the last 7 days. • Unapproved changes in the past 7 days. • ACLs identified. • ACLs in use. • ACL changes in the past 7 days.
III.A. Involve the Board of Directors	Displays the number of: • Available user reports. • Available System reports.
III.B. Assess Risk	Displays the number of: • Configuration management “Best Practices” green status. • Devices software level. • Monitors with an “Okay” status. • Devices with access failures. • Devices with port availability of less than 10%. • Devices with different startup and running configurations.
III.C.1. Manage and Control Risk (Policies & Procedures)	Displays the number of: • Workflow rules in place. • Configuration policies in place. • Device password rules in place.
III.C.2. Manage and Control Risk (Training)	You can access the following documentation: • *NA User Guide* • *NA Release Notes*

Fields	Description/Action
III.C.3. Manage and Control Risk (Testing)	Displays the number of: • Configuration policy non-compliance events in the past 24 hours. • Configuration policy non-compliance events in the past 7 days. • Devices not in software level. • Diagnostics run in the past 24 hours. • Diagnostics run in the past 7 days.
III.D. Oversee Service Provider Arrangements	Displays the number of: • Stored configurations. • Devices with different startup and running configurations. • Non-active devices. • Devices with access failures.
III.E. Adjust the Program	Displays the number of: • Users added in the last month. • Devices added in the last month. • Device groups added in the last month. • Configuration stored in the last month.
III.F. Report to the Board	Displays: • The number of Configuration management “Best Practices” green status. • System Status report. • Summary reports. • HP Network Automation Compliance Center.
III.G. Implement the Standards	This requirement is outside the scope of NA.

HIPAA Compliance Status Reports

HIPAA is the Health Insurance Portability & Accountability Act of 1996. The final HIPAA Security Rule was published on February 20, 2003. Under the final rule, covered entities include the Department of Health and Human Services (HHS) Medicare Program, other federal agencies operating health plans or providing health care, state Medicaid agencies, private health plans, health care providers, and health care clearinghouses that process, transmit, and/or store protected health information (PHI) in electronic form.

For detailed information on HIPAA, click the “More information about HIPAA and achieving compliance using HP Network Automation” link.

To view the HIPAA Compliance Status reports:

1. On the menu bar under Reports, click Compliance Center. The Compliance Center Home page opens.
2. Click the HIPAA Compliance Status link. The HIPAA Compliance Status page opens.

HIPAA Compliance Status Page Fields

Fields	Description/Action
Security Standards: General Rules	
(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.	Displays the number of: • Stored device configurations • Devices with access failures. • Devices with port availability of less than 10%.
(2) Protect against any reasonably-anticipated threats or hazards to the security or integrity of such information.	Displays the number of: • Failed user login attempts in the past 7 days. • ACLs identified. • ACLs in use. • ACL changes in the past 7 days.
(3) Protect against any anticipated uses or disclosures that are not permitted or required under subpart E of this part.	Displays the number of: • Users restricted to specific sets of devices. • Users assigned Administrator access permissions.
(4) Ensure compliance with this subpart by its workforce.	You can open the HP Network Automation Compliance Center HIPAA Compliance Status report.

Fields	Description/Action
Administrative Safeguards	
(A) Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.	Displays the number of: • Configuration management “Best Practices” green status. • Devices in software level. • Monitors with an “Okay” status. • Devices with access failures. • Devices with port availability of less than 10%. • Software vulnerabilities detected. • Devices with different startup and running configurations.
(B) Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).	Displays the number of: • Workflow rules in place. • Active configuration policies. • Device Password Rules in place.
(C) Sanction policy (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.	This requirement is outside the scope of NA.
(D) Information system activity review (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Displays the number of: • User login attempts in the past 7 days. • Users added in the past 7 days. • Users deleted in the past 7 days. • User permissions changed in the past 7 days. • Configuration policies changed in the past 7 days. • Configuration policies added in the past 7 days.
Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.	This requirement is outside the scope of NA.
Workforce Security	
(A) Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	Displays the number of: • Users restricted to specific group of devices. • Approved changes in the last 7 days. • Unapproved changes in the last 7 days.
(B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Displays the number of users assigned Administrator Access permissions.

Fields	Description/Action
(C) Termination procedures (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	Displays the number of users deleted in the past 7 days.
Information Access Management	
(A) Isolating health care clearinghouse functions (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	Displays the number of: • Users restricted to specific groups of devices. • Users assigned restricted (non-Admin) access permissions.
(B) Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	Displays the number of: • Users restricted to specific groups of devices. • Users assigned restricted (non-Admin) access permissions.
(C) Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Displays the number of: • User accounts enabled in HP Network Automation. • User accounts disabled in HP Network Automation.
Security Awareness and Training	
(A) Security reminders (Addressable). Periodic security updates.	Displays the number of: • User accounts enabled in HP Network Automation • User accounts disabled in HP Network Automation.
(B) Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.	This requirement is outside the scope of NA.
(C) Log-in monitoring (Addressable). Procedures for monitoring log-in attempts and reporting discrepancies.	Displays the number of: • User login attempts in the past 7 days. • Failed user login attempts in the past 7 days.
(D) Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.	Displays the number of NA password changes in the past 7 days.
Security Incident Procedures	
Response and Reporting (Required). Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.	Displays the number of: • User login attempts in the past 7 days. • Failed user login attempts in the past 7 days. • Configuration changes detected in the past 7 days.

Fields	Description/Action
Contingency Plan	
(A) Data backup plan (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	NA does not create or maintain electronic protected health information.
(B) Disaster recovery plan (Required). Establish (and implement as needed) procedures to restore any loss of data.	NA is a high-availability (HA) system that can be implemented to support automatic failure detection and automatic (or manual) failover with no data loss.
(C) Emergency mode operation plan (Required). Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	NA is a high-availability (HA) system that can be implemented to support automatic failure detection and automatic (or manual) failover with no data loss.
(D) Testing and revision procedures (Addressable). Implement procedures for periodic testing and revision of contingency plans.	NA supports periodic testing of automatic failure detection and automatic (or manual) failover.
(E) Applications and data criticality analysis (Addressable). Assess the relative criticality of specific applications and data in support of other contingency plan components.	NA's robust reporting capabilities provide the foundation to assess NA' relative criticality with respect to other contingency plan components.
Evaluation	
Perform a periodic technical and nontechnical evaluation.	Displays the number of: • Users restricted to specific group of devices. • Users assigned Administrator Access permissions. • Workflow rules in place. Clicking the Workflow Setup page opens the Workflow Wizard. • Configuration policies in place. • Device password rules in place.
Written contract or other arrangement (Required). Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).	This requirement is outside the scope of NA.
Physical Safeguards	
(i) Contingency operations (Addressable). Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	This requirement is outside the scope of NA.

Fields	Description/Action
(ii) Facility security plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	This requirement is outside the scope of NA.
(iii) Access control and validation procedures (Addressable). Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	Displays the number of: • User login attempts in the past 7 days. • Failed user login attempts in the past 7 days. • Users restricted to specific groups of devices. • Users assigned restricted (non-Admin) access permissions.
(iv) Maintenance records (Addressable). Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	This requirement is outside the scope of NA.
Workstation Use	
Implement policies and procedures that specify the proper functions to be performed.	This requirement is outside the scope of NA.
Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	This requirement is outside the scope of NA.
Device and Media Controls	
(i) Disposal (Required). Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	This requirement is outside the scope of NA.
(ii) Media re-use (Required). Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.	This requirement is outside the scope of NA.
(iii) Accountability (Addressable). Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	This requirement is outside the scope of NA.
(iv) Data backup and storage (Addressable). Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	This requirement is outside the scope of NA.
Technical Safeguards	
(i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.	Displays the number of: • User accounts enabled in HP Network Automation. • User accounts disabled in HP Network Automation.

Fields	Description/Action
(ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	HP Network Automation is a high-availability (HA) system that can be implemented to support automatic failure detection and automatic (or manual) failover with no data loss.
(iii) Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Web user sessions terminated after 1800 seconds of inactivity. 1800 is the default value. This value can be configured.
(iv) Encryption and decrypting (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.	This requirement is outside the scope of NA.
Audit Controls	
Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	This requirement is outside the scope of NA.
Standard Integrity	
Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	This requirement is outside the scope of NA.
Person or Entity Authentication	
Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	This requirement is outside the scope of NA.
Transmission Security	
(i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	This requirement is outside the scope of NA.
(ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	This requirement is outside the scope of NA.
Policies and Procedures	
Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements.	This requirement is outside the scope of NA.

Fields	Description/Action
Documentation	
(i) Time limit (Required). Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	This requirement is outside the scope of NA.
(ii) Availability (Required). Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	This requirement is outside the scope of NA.
(iii) Updates (Required). Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	This requirement is outside the scope of NA.

PCI Data Security Standard Compliance Status Reports

In an effort to combat data theft and maintain consumer confidence, all of the major credit card issuers have formulated detailed security programs, including:

- Visa USA Cardholder Information Security Program (CISP)
- MasterCard Site Data Protection (SDP) program
- Discover Information Security and Compliance (DISC) program
- American Express Data Security Operating Policy (DSOP)

In late 2004, Visa and MasterCard aligned their programs under a single standard: the Payment Card Industry (PCI) Data Security Standard. Fundamental security best practices focused on protecting cardholder data comprise the 12 PCI requirements. Penalties for failure to comply with the requirements or to rectify a security issue are severe: possible restrictions on the merchant or permanent prohibition of the merchant’s participation in Visa programs, and a fine of up to $500,000 per incident.

For information about the ways that NA functionality pertains to the PCI Data Security Standard, click the “More information about the PCI Data Security Standard and achieving compliance using HP Network Automation” link.

To view the PCI Data Security Standard Compliance Status reports:

1. On the menu bar under Reports, click Compliance Center.

   The Compliance Center Home page opens.

2. Click the PCI Data Security Standard Compliance Status link.

   The PCI Data Security Standard Compliance Status page opens.

PCI Data Security Standard Compliance Status Page

The PCI Data Security Standard Compliance Status page consolidates information available in NA under the requirements of the PCI Data Security Standard. For each standard requirement, the page presents a table with the following columns:

- **Specification**—Each row in the table describes one portion of the requirement.
- **Status**—Displays a summary of the managed network as it applies to this portion of the requirement.
- **More Information**—Links to the NA console pages that support the information in the Summary column.

Chapter 19: Creating Workflows

Use the following table to quickly locate information.

Topic	Refer to:
Getting Started	"Getting Started" on page 670
Workflow Wizard	"Workflow Wizard" on page 671
My Tasks	"My Tasks" on page 673
Approval Requests	"Approval Requests" on page 676
Approving Tasks	"Approving Tasks" on page 678
Email Notification	"Email Notification" on page 681

Getting Started

The HP Network Automation (NA) Workflow Integration & Routing Engine (WIRE) manages the process of network configuration, ensuring that network changes are made according to predefined policies, completed in the correct sequence, and approved by the appropriate people.

By controlling who does what to the network and why, device configurations can be accomplished accurately and in accordance with the objectives of your organization. Because Workflow manages the sequencing of tasks, the gaining of approvals, and the auditing of results, out-of-policy changes and inadvertent configuration errors are far less likely to occur.

The following terms are used in this chapter.

- Task — Tasks are the primary mechanism by which NA interacts with your network. Tasks are specific actions you can either schedule or run immediately. Completed tasks provide the result of NA activities. Workflow tasks include all tasks, for example:
  - Deploy Passwords
  - Reboot Device
  - Task Snapshot
  - Run Command Script
  - Synchronize Startup and Running Configurations
  - Update Device Software
  - Run Diagnostics

  For a complete list of tasks, refer to “What Are Tasks?” on page 279.
- Project — A project is an ordered sequence of tasks. From NA’s point of view, a project is just another type of task with sub-tasks that are sequentially run (instead of in parallel).
- Originator — An individual who submits a task for approval.
- Approver — An individual or a group of individuals who can approve a task and confirm that the task complies with all internal policies.
- FYI Recipients — An individuals or a group of individuals who receive notification based on actions taken by the originator or the approver.
- Approved — The approval status of a task that has been approved for execution.
- Not Approved — The approval status of a task that has been rejected. A rejected task either does not have enough data or has incorrect data that could lead to negative consequences on the network. A rejected task cannot be recycled.
- Suspended — The approval status of a task that is temporarily (or permanently) on hold.

- Override — An action performed by the Originator of a task for use in emergencies when the approval process needs to be overridden. This function is only available if enabled in the Administrative Settings.

Note: You may want to enable all Power users to create tasks that do not require approval. Refer to "Workflow Wizard" on page 671 for information on creating rules. For example, you can create a rule, "All Power Users do not need approval," before a "All Users need approval by Admin" rule to enable Power users to bypass approval.

Workflow Wizard

The Workflow Wizard enables you to easily setup a Workflow for tasks. To open the Workflow Wizard, on the menu bar under Admin click Workflow Setup. The Workflow Wizard opens.

Step	Description/Action
Welcome Page	The Welcome page provides a brief introduction to the Workflow Wizard. Click Next to continue.
Step 1: Enable Workflow	You are asked if you want to enable Workflow and require approval for some or all tasks. Click Yes and then click Next to continue. If you click No and then click Next, the Setup Complete page opens, where you can return to Workflow Wizard home page.
Step 2: Enable Workflow - Cont'd.	The Enable Workflow - Cont'd page provides an overview of the information you must provide when creating a Workflow. Click Next to continue.
Step 3: Manage Approval Rules	Enter the name of the new Workflow Approval Rule and click Next to continue. You also have the option of modifying or deleting existing Workflow Approval Rules. All existing Workflow Approval Rules are displayed at the bottom of the page. (**Note**: NA is shipped with one default Workflow Approval Rule: *All users approved by Administrator.*) **Note**: Workflow Approval Rules can be partitioned according to Partitions. Keep in mind that there are some Workflow Approval Rules that are available to all Partitions. These Workflow Approval Rules are labeled "Shared" (or "Global"), depending on configuration. However, you cannot edit or delete them without proper permissions. For information on creating Partitions, refer to "Segmenting Devices and Users" on page 150.
Step 4: Originator Setup	The Originator Setup page enables you to designate the users that will trigger this rule when they create a task. When you are done adding users, click Next to continue.
Step 5: Task Setup	The Task Setup page enables you to designate which tasks need approval. When you are done adding tasks, click Next to continue. If you do not designate a task to require approval, the approval setting for that task appears as "Not Applicable."

Step	Description/Action
Step 6: Device Group Setup	The Device Group Setup page enables you to define Workflow Approval Rules based on device groups. This enables you to configure Workflow Approval Rules on device usage, device type, and so on. If device partitioning is enables, there is a Partition selection drop-down menu. Keep in mind that the priority level can only adjusted inside a Partition. Global rules always have higher priority than Partition rules. When you are done adding device groups, click Next. Keep in mind that at task creation time, the Workflow Approval Rule only applies if: • The task is against a single device and the Workflow Approval Rule's device group contains the device. • The task is against a device group and the Workflow Approval Rule’s device group has a non-empty intersection with the task’s device group.
Step 7: Approver Setup	The Approver Setup page enables you to designate who can approve a task and confirm that the task complies with all internal policies, or if no approval is required. Keep in mind that a task originator cannot review his/her own tasks. When you are done adding users, click Next to continue.
Step 8: FYI Recipient Setup	The FYI Recipient Setup page enables you to designate who receives notification based on actions taken by the Workflow Approval Rule originator or approver. When you are done adding users, click Save. Keep in mind that originators and approvers need not be added as recipients. Refer to “Email Notification” on page 681 for detailed information on email notification.
Setup Complete	After you have successfully added a Workflow Approval Rule, the “Successfully created new rule <rule name>” message is displayed at the top of the page. You can now create a new Workflow Approval Rule for other users (originators) or modify/delete existing approval rules by clicking the Manage Approval Rules link. You can click the My Tasks option from the Tasks drop-down menu to view a summary of originator and approver actions. Refer to “My Tasks” on page 673 for information.

My Tasks

The My Tasks page shows tasks originated by the current logged in user, including the task approval status, if applicable, and if the task has not yet run.

To view the My Tasks page, on the menu bar under Tasks click My Tasks. The My Tasks page opens.

My Tasks Page Fields

Field	**Description/Action**
My Drafts link	If applicable, opens the My Drafts page.
Approval Requests link	If the task requires approval, opens the Approval Requests page, where you can view tasks needing approval by the currently logged in user. By default, the page shows tasks that have not completed, including tasks that are: • Not approved • Waiting Approval • Waiting to run Refer to "Approval Requests" on page 676 for information.
Scheduled Tasks link	Opens the Scheduled Tasks page, where you can view scheduled tasks that are in the queue, but have not yet run. Refer to "Scheduled Tasks Page Fields" on page 402 for information.
Running Tasks link	Opens the Running Tasks page, where you can view all running tasks. Refer to "Running Tasks Page Fields" on page 404 for information.
Recent Tasks link	Opens the Recent Tasks page, where you can view all recent tasks. Refer to "Recent Tasks Page Fields" on page 406 for information.
Show Tasks Check Boxes	If the task requires approval, you can select the following display options: • Approved • Not Approved • Waiting Approval • Overridden • Draft • No Approval Required
Check Boxes	You can use the left-side check boxes to delete tasks. Once you have selected the tasks, click the Actions drop-down menu and click Delete. The adjacent Select drop-down menu enables you to select or deselect all tasks.
Schedule Date	Displays the date and time the task was created.
Task Name	Displays the task name. Clicking a task opens the Task Information page. Refer to "What Are Tasks?" on page 279 for information on Tasks.

Field	Description/Action
Approved By Date	If applicable, displays the date and time the task must be approved. If a task is not approved by its approval date, its status is set to “Not Approved.” (**Note**: Approval options are only displayed if the task is part of a Workflow Approval Rule.)
Approval Status	If applicable, displays the task’s approval status. Approval status is only displayed if the task is part of a Workflow Approval Rule. Approval statuses include: • Awaiting Approval • Approved • Not Approved • Overridden • No Approval Required
Task Status	Displays the status of the task. Statuses include: • Warning — A group task containing some failed sub-tasks, but not all tasks failed. • Draft — NA will not run the task, nor is the task sent out for approval, when in Draft status. • Duplicate — The task was not started because an identical task is already running. • Failed — The task failed. • Paused — Someone paused the task. It will not run when its scheduled time arrives. • Pending — The task is queued and waiting for its scheduled time. • Running — The task has started, but has not yet finished. • Skipped — The task was skipped due to errors, for example incorrect permissions, unmanaged devices, and so on. • Succeeded — The task succeeded. • Waiting — Although the scheduled time has arrived, the task is waiting because the “Max Concurrent Tasks” limit has been reached.
Priority	Displays the task’s priority. Refer to “Scheduling Tasks” on page 280 for information on task priority.
Task Type	Displays the task type, for example: • Deploy Password • Deploy Config • Discover Driver • Reboot Device • Take Snapshot • Synchronize Startup and Running Configurations For a complete list of tasks, refer to “What Are Tasks?” on page 279. (**Note**: Multi-Task Project tasks may or may not be displayed on the My Tasks results page. It depends on whether the Multi-Task Project task includes at least one of the task types listed above as a sub-task.)

Field	Description/Action
Actions	You can select one of the following options: • Delete — Enables you to delete the task. • Pause — Pauses the task so it does not run at its scheduled time. (**Note**: You can select Resume if you want to resume the task.) • Run Now — Runs the task as soon as possible. If the maximum number of concurrent tasks has not been reached, the task runs immediately. • Edit — Opens the Edit Task page for that task.
Display results in groups of	You can set the number of items to display per page from the drop-down menu. The default is 25.

Approval Requests

The Approval Requests page enables you to view tasks needing approval by the currently logged in user. By default, the page shows tasks that have not yet completed where the approval status is either Approved, Waiting Approval or Not Approved.

Note: To view completed tasks, on the menu bar under Reports, select Search For and click Tasks. Refer to "Search For Task Page Fields" on page 504 for information.

To view the Approval Requests page, on the menu bar under Tasks, click Approval Requests. The Approval Requests page opens.

Approval Requests Page Fields

Field	Description/Action
My Tasks	Opens the My Tasks page, where you can view the status of each task. Refer to "My Tasks Page Fields" on page 673 for information.
Scheduled Tasks link	Opens the Scheduled Tasks page, where you can view scheduled tasks that are in the queue, but have not yet run. Refer to "Scheduled Tasks Page Fields" on page 402 for information.
Running Tasks link	Opens the Running Tasks page, where you can view all running tasks. Refer to "Running Tasks Page Fields" on page 404 for information.
Recent Tasks link	Opens the Recent Tasks page, where you can view all recent tasks. Refer to "Recent Tasks Page Fields" on page 406 for information.
Show Tasks	If checked, tasks with the following approval status are displayed: • Approved • Not Approved • Waiting Approval
Task Name	Displays the task name. To approve a task, click the Task name. The Task Information page opens. Refer to "Task Information Page Fields" on page 678 for information.
Approve By	Displays the date and time the task must be approved. If a task is not approved by its approval date, its status is set to "Not Approved." (**Note**: Tasks that have run are removed from the Approval Request page. Tasks past their approval date are marked Not Approved and will remain on the Approval Request page until the Data Pruner deletes them. Refer to "Data Pruning Task Page Fields" on page 387 for information on data pruning.)
Approval Status	Displays the task's approval status. Approval statuses include: • Waiting Approval • Not Approved
Priority	Displays the task's priority.
Date	Displays the date and time the task was created.

Field	Description/Action
Status	Displays the status of the task. Statuses include: • Warning — A group task containing some failed tasks, but not all tasks failed. • Draft — NA will not run the task, nor is the task sent out for approval, when in Draft status. • Duplicate — The task was not started because an identical task is already running. • Failed — The task failed. • Paused — Someone paused the task. It will not run when its scheduled time arrives. • Pending — The task is queued and waiting for its scheduled time. • Running — The task has started, but has not yet finished. • Skipped — The task was skipped due to errors, for example incorrect permissions, unmanaged devices, and so on. • Succeeded — The task succeeded. • Waiting — Although the scheduled time has arrived, the task is waiting because the “Max Concurrent Tasks” limit has been reached.
Scheduled By	Displays the name of the person who scheduled the task.

Approving Tasks

If you have been designated to approve a task:

1. On the menu bar under Tasks, click Approval Requests. The Approval Requests page opens. Refer to "Approval Requests Page Fields" on page 676.
2. Click the task name to view approval options. The Task Information page opens.
3. Click the Approve button.

Task Information Page Fields

The Task Information page includes detailed information on tasks, including:

- Task status
- Originator
- Devices affected
- Duration
- Approval information
- Result details

The Task information page also provides links to more detailed information in the event of a warning or failure. Keep in mind that a task can be successfully completed but still contain errors. For example, you could successfully deploy to a running configuration but have invalid commands within the configuration.

To open the Task Information page:

1. Select a device from the Inventory page. The Device Details page opens.
2. From the View drop-down menu, click Device Tasks. The Device Tasks page opens.
3. Click the Detail option in the Actions column for the task on which you want detailed information. The Task Information page opens.

Field	Description/Action
Edit Task link	Opens the task page so that you can edit the task. This link is only displayed for pending tasks.
Run Again link	Opens the task page so that you can re-run the task. This link is only displayed for completed tasks.
Return to List link	Opens the My Tasks page. Refer to "My Tasks Page Fields" on page 399.
General Information	
Task Name	Displays the task name.

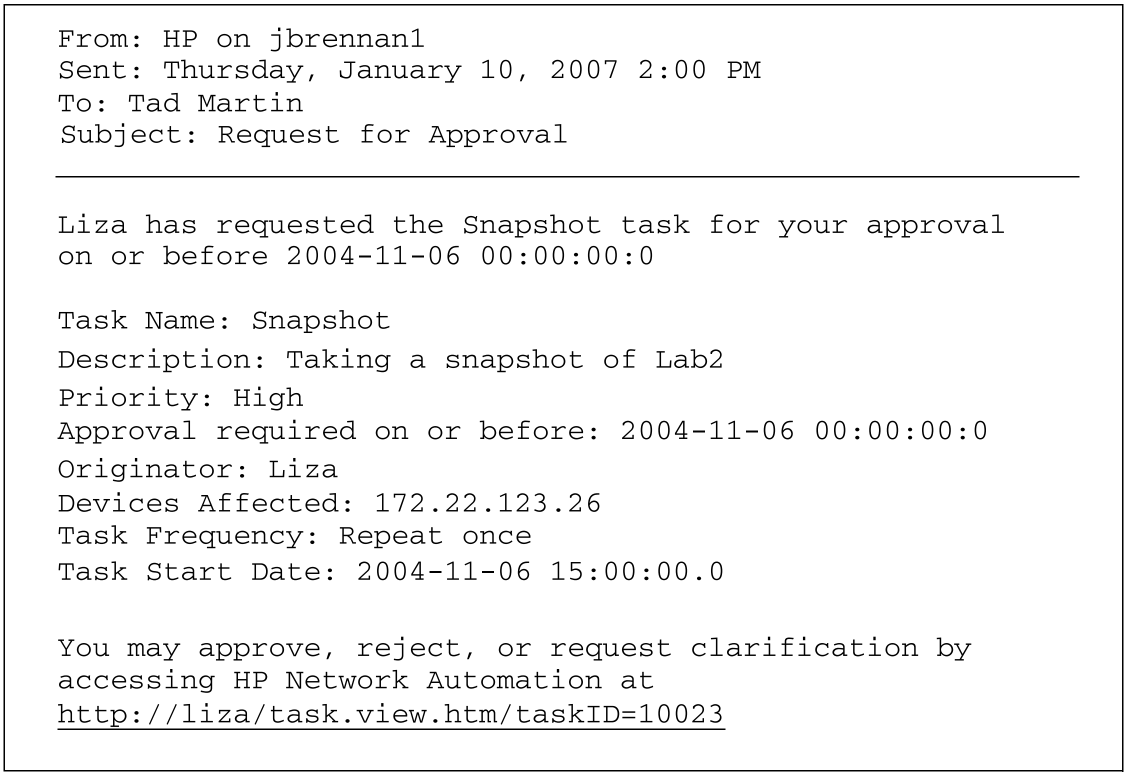
Field	Description/Action
Task Status	Displays the task status, including: • Draft • Duplicate • Failed • Paused • Pending • Requested (Note: Requested means the task is waiting for Approval. Refer to "Approving Tasks" on page 678.) • Running • Skipped • Succeeded • Synchronous (Note: NA typically runs tasks by creating a thread and letting the task run asynchronously in the background. The CLI and API enable synchronous tasks where they are run in the current thread and the command blocks until the command completes.) • Waiting • Warning **Note**: Multi-task projects will continue processing when a warning is encountered. The warning status is shown in the parent task.
Comments	Displays any comments about the task.
Originator	Displays the username or process that scheduled the task.
Create Date	Displays the date and time the task was created.
Devices Affected	Displays the host name and/or IP address of the affected device.
Schedule Date	Displays the date and time the task was scheduled to run.
Start Date	Displays the task's start date.
Complete Date	Displays the task's complete date.
Duration	Displays the task's duration.
Repeat Type	Displays the repeat type, for example: non-recurring.
Approval Information	
Approver(s)	Displays a list of task approvers.
Approval Status	Displays the task approval status.
Priority	Displays the task priority.
Approved By	Displays the date and time the task must be approved.
New Comments	Enter additional comments about the task.
Approve Button	Click the Approve button to approve the task.

Field	Description/Action
View Task Details link	Clicking the View Tasks link opens the Diagnostics History page.
Additional Information	
Result Details	Displays the diagnostics that were automatically run (depending on the device type), for example: • Diagnostic “NA Module Status” completed • Diagnostic “NA Routing Table” completed • Diagnostic “NA OSPF Neighbors” completed
Task History	
Task History Information	Displays task history information, such as when the task was run, the repeat type, and status.

Email Notification

Task approvers receive email notification based on actions taken by the Workflow Rule originator. The Workflow Wizard’s FYI Recipient Setup page can be used to notify users other than approvers of the task. Refer to “Workflow Wizard” on page 671.

A sample email notification is shown below.



```
From: HP on jbrennan1
Sent: Thursday, January 10, 2007 2:00 PM
To: Tad Martin
Subject: Request for Approval
________________________________________________________

Liza has requested the Snapshot task for your approval
on or before 2004-11-06 00:00:00:0

Task Name: Snapshot
Description: Taking a snapshot of Lab2
Priority: High
Approval required on or before: 2004-11-06 00:00:00:0
Originator: Liza
Devices Affected: 172.22.123.26
Task Frequency: Repeat once
Task Start Date: 2004-11-06 15:00:00.0

You may approve, reject, or request clarification by
accessing HP Network Automation at
http://liza/task.view.htm/taskID=10023
```

Clicking the link at the bottom of the email opens the Approval Requests page where you can approve or not approve a task. Refer to “Approval Requests Page Fields” on page 676.

Chapter 20: Working With ACLs

Use the following table to quickly locate information.

Topic	Refer to:
Getting Started	"Getting Started" on page 684
Viewing ACLs	"Viewing ACLs" on page 685
Running Command Scripts	"Running Command Scripts" on page 689
Creating ACLs	"Creating ACLs" on page 690
Changing ACL Applications	"Changing ACL Applications" on page 691
Batch Inserting ACL Lines	"Batch Inserting ACL Lines" on page 692
Batch Deleting ACL Lines	"Batch Deleting ACL Lines" on page 692
Commenting ACLs and Creating ACL Handles	"Commenting ACLs and Creating ACL Handles" on page 694
Creating ACL Templates	"Creating ACL Templates" on page 695
Editing ACLs	"Editing ACLs" on page 696
Deleting ACLs	"Deleting ACLs" on page 697

Getting Started

Access Control Lists (ACLs) are used by many organizations to control the flow of IP traffic. This is done mostly for increased security, but can also be used to increase performance by preventing the operation of bandwidth intensive systems, such as streaming audio or video, from public Web sites.

In general, the definition of an ACL is a collection of configuration statements. These statements define addresses and/or patterns to accept or deny. NA retrieves configuration information from devices and extracts the ACL statements from the configuration. NA then stores the ACLs independent of the configuration.

The NA ACL Manager provides a quick way to:

- View ACLs on devices
- Maintain a history of ACLs
- Comment on ACLs and maintain those comments in the configuration

The ACL Manager also provides a quick way to use existing ACL configurations to create ACL templates.

This chapter includes instructions on how to enable (and disable) ACLs parsing for a device or group of devices.

- For information on turning on ACL parsing for a single device, refer to "Configuration Mgmt Page Fields" on page 38.
- For information on turning on ACL parsing for a group of devices, refer to "Batch Edit Device Page Fields" on page 163.
- For information on searching for ACLs, refer to "Search For ACLs Page Fields" on page 528.

Note: ACL information is not available until after the first stored or checkpoint snapshot is taken of the device after ACL parsing is enabled.

Viewing ACLs

To view ACLs on a device:

1. On the menu bar under Devices, click Inventory.
2. On the Inventory page, select the device that has ACL parsing enabled. The Device Details page opens. (Note: When adding devices that support ACLs, make sure the Enabled option is selected.) Once the devices are discovered, and a checkpoint snapshot is taken, you are able to view a device's ACLs. (Refer to "Adding Devices" on page 108 for more information on adding devices.)
3. From the View drop-down menu, select Device Detail and then click ACLs. The Device ACLs page opens. Refer to "Device ACLs Page Fields" on page 685.
4. On the Device ACLs page, click the View ACL option for any ACL listed. The View ACL page opens. Refer to "View ACL Page Fields" on page 687.

Device ACLs Page Fields

Field	Description/Action
Hostname	Displays the device's host name. Clicking the device's host name opens the last visited Device Details page, where you can view information about this device's ACLs.
Device IP	Displays the device's IP address. Clicking the device's IP address opens the last visited Device Details page, where you can view information about this device's ACLs.
Last Snapshot Attempt	Displays the date and time of the last snapshot attempt.
Last Snapshot Result	Displays the last snapshot result, for example "Configuration Change Detected."
Check Boxes	You can use the left-side check boxes to compare two ACLs. Once you have selected the ACLs, click the Actions drop-down menu and click: • Compare — Opens the Compare Script page, where you can compare the two selected ACLs side by side. The differences are highlighted in different colors to make them easy to view. The adjacent Select drop-down menu enables you to select or deselect all of the device configurations.
ACL ID	Displays the ACL ID. The ACL ID refers to how the device identifies the ACL in its configuration. Keep in mind that while many devices use an integer index as the ACL ID, not all do. As a result, ACL IDs are stored as strings.
ACL Handle	Displays the ACL handle. The ACL Handle is the ACL name you defined. By default, the ACL Handle is the same as the ACL ID. If you do not supply a specific ACL Handle, the driver uses the ACL ID. (Note: This field is used to sort ACLs by default.)
ACL Type	Displays the ACL type, as defined by the device.
Last Modified Date	Displays the date and time the ACL was last modified.

Field	Description/Action
Actions	You can select the following actions: • Edit ACL — Opens the Edit ACL page, where you can edit the ACL. Refer to "Running Command Scripts" on page 689 for information. • View ACL — Opens the View ACL page, where you can view the ACL. Refer to refer to "View ACL Page Fields" on page 687 for information. • ACL History — Opens the ACL History page, where you can view the full audit trail of all changes. Keep in mind that you can use the ACL history to facilitate restoring an ACL to a prior configuration. To do this, you would view the historical ACL and then click the Edit ACL action link.

View ACL Page Fields

To open the View ACL page:

1. On the menu bar under Devices, click Inventory.
2. On the Inventory page, select the device that has ACL parsing enabled. The Device Details page opens. (Note: When adding devices that support ACLs, make sure the Enabled option is selected.) Once the devices are discovered, and an initial snapshot is taken, you are able to view a device' ACLs.
3. From the View drop-down menu, select Device Detail and then click ACLs. The Device ACLs page opens.
4. On the Device ACLs page, click the View ACLs option for any ACL listed. The View ACL page opens.

Field	Description/Action
Device	Display the host name and IP address of the device. Clicking the device's IP address opens the last visited Device Details page, where you can view information about this device's ACLs.
ID	Displays the ACL ID. The ACL ID refers to how the device identifies the ACL in its configuration.
ACL Handle	Displays the ACL handle. The ACL Handle is the ACL name you defined.
ACL Type	Displays the ACL type.
Last Modified Date	Displays the date and time the ACL was last modified.
Last Modified User	Displays the user who last modified the ACL. Keep in mind that the last modified user can be "N/A" to indicate that NA does not know which user is responsible for this particular version of the ACL. If a user is shown, a link to the User Attribution Details page is provided, showing all activity NA knows about that occurred prior to retrieving this version of the ACL. Because the user is only NA's best guess, it is possible that other activity represents the actual cause for the ACL change.
ACL Script	Displays the configuration scripting that defines the ACL. The ACL script represents the configuration lines necessary to define the ACL. You can select the following options: • New ACL — Opens the Run Command Script Task page, enabling you to use the existing ACL as a template. (Refer to "Creating ACLs" on page 690.) • Edit ACL — Opens the Run Command Script Task page, enabling you to edit the ACL. (Refer to "Running Command Scripts" on page 689.) • New ACL Template — Opens the New Command Script page, enabling you to save the existing ACL as a template. (Refer to "Creating ACL Templates" on page 695.) • Edit ACL Template — Opens the New Command Script page, enabling you to create a template that edits the current ACL. (Refer to "Creating ACL Templates" on page 695.)

Field	Description/Action
ACL Application	If the ACL is applied, the ACL application is displayed. ACL applications include a list of configuration commands that define where the ACL is used. Keep in mind that some ACL types do not have any separate application scripting. These ACLs will not show any application script. You can select the following options: • Apply ACL — Opens the New Task - Run Command Script page, enabling you to (re) apply the ACL. (Refer to “Creating ACLs” on page 690.) • Apply ACL Template — Opens the New Command Script page, creating an ACL application template. (Refer to “Creating ACL Templates” on page 695.)
Comments	Displays any comments about the ACL. You can select the following options: • Edit Comments — Opens the Edit ACL Page. • History — Opens the ACL History page. • View Related Config — Opens the Device Configuration page. (Refer to “Device Configuration Detail Page Fields” on page 177.)

Running Command Scripts

The Run Command Script task enables you to run command scripts. Refer to "Run Command Script Task Page Fields" on page 306 for information. Keep in mind that on the Run Command Script Task page, the following Task Options are shown:

- Command Script to Run — Indicates that you are running an ACL Edit Script from a specific ACL on the device. The ACL is identified both by its ID and Handle (in parentheses).
- Limit to script types — The script type is automatically set to "ACL Edit Script."
- Mode — Displays the device access mode, such as Cisco IOS configuration.
- Script — Displays the device-specific commands to run. The script to run is automatically populated, providing a copy of the existing ACL configuration. Keep in mind that if you are editing an ACL with applications, you will be provided with copies of the ACL application scripting, both before the ACL configuration scripting (to undo applications, if necessary) and after the ACL configuration scripting (to reapply the ACL). In many cases (such as IOS), to make an ACL configuration exactly match what you specify in a script, you will need to remove that ACL first, then put it back.

Creating ACLs

To create a new ACL using an existing ACL as a template:

1. On the menu bar under Devices, click Inventory.
2. Select the device whose ACL parsing you want to enable. The Device Details page opens.
3. From the View drop-down menu, select Device Detail and click ACLs. The Device ACLs page opens.
4. In the Actions column, click the Edit ACL option. The Run Command Script page opens. Refer to “Run Command Script Task Page Fields” on page 306 for information.

The following fields in the Run Command Script Task page are automatically populated:

- Command Script to Run — Displays the type of script (Apply ACL) and the source ACL.
- Limit to script types — Displays the type of script (ACL Edit Script).
- Mode — Displays the correct script mode for applying an ACL on the device.
- Script — Displays a copy of the existing ACL application scripting. Be sure to check this thoroughly and make any necessary changes.

Note: You should not run ACL scripts line-by-line. ACL scripts can result in lost connectivity when run line-by-line.

If you add an ACL to a device using the same ACL ID that already exists, you are actually editing the existing ACL on that device.

Changing ACL Applications

To change ACL applications:

1. On the menu bar under Devices, click Inventory.
2. Select the device whose ACL parsing you want to enable. The Device Details page opens.
3. From the View drop-down menu, select Device Detail and click ACLs. The Device ACLs page opens.
4. Click the View ACL option. The View ACL page opens. (Refer to "View ACL Page Fields" on page 687.)
5. Click the Apply ACL option. The Run Command Script page opens. (Refer to "Creating ACLs" on page 690.)

The following fields in the Run Command Script Task page are automatically populated:

- Command Script to Run — Displays the type of script (Apply ACL) and the source ACL.
- Limit to script types — Displays the type of script (ACL Application Script).
- Mode — Displays the correct script mode for applying an ACL on the device.
- Script — Displays the copy of the existing ACL application scripting.

Note: You should not run ACL scripts line-by-line. ACL scripts can result in lost connectivity when run line-by-line.

Batch Inserting ACL Lines

You can batch deploy ACL lines. NA automatically adds the necessary lines to the appropriate ACL on single or multiple devices, based on ACL ID or ACL Handle. The following steps are specific to Cisco IOS devices only.

To batch insert a line into an ACL(s)

1. On the menu bar under Devices, select Device Tasks and click Batch Insert ACL Line. The New Task - Run Command Script page opens. (Refer to "Creating ACLs" on page 690.)
2. You can select a device or group of devices on which to run the task. Upon selecting device or group, the page will update.
3. Command Script to Run — Choose either:
   a) Cisco IOS Insert Line into ACL by ACL ID
      - Id of ACL to insert line into — Enter the ACL ID that you want to add a line to. If you selected a group of devices, this adds a line to each device that contains an ACL that matches this ACL ID.
      - ACL line to insert — Enter the ACL line exactly as you would on the device.
      - Location to add line — Choose where to add the line. Options include first, last, and next-to-last.
      - Update Scripts — Click when you have completed the above variables.
      - Parameters — Optional parameters.
      - Script — This is the actual script that updates the ACL. The option to edit this script before execution makes this feature very flexible.

   b) Cisco IOS Insert Line into ACL by Handle
      - ACL Handle — Enter the ACL Handle that you want to add a line to. If you selected a group of devices, this will add a line to each device that contains an ACL that matches this ACL Handle.
      - ACL line to insert (without 'access-list {id}') — Enter the ACL line that you want to insert without any "access-list ACLID." The script will place this if necessary.
      - Location to add line — Choose where to add this line. Options include first, last, and next-to-last.
      - Update Scripts — Click when you have completed the above variables.
      - Parameters — Optional parameters.
      - Script — This is the actual script that will update the ACL. The option to edit this script before execution makes this feature very flexible.

Batch Deleting ACL Lines

You can batch remove ACL lines. NA automatically removes the necessary lines to the appropriate ACL on single or multiple devices, based on the ACL ID or ACL Handle. The following steps are specific to Cisco IOS devices only.

To batch delete a line into an ACL(s)

1. On the menu bar under Devices, select Device Tasks and click Batch Remove ACL Line. The New Task - Run Command Script page opens. (Refer to "Creating ACLs" on page 690".)
2. You can select a device or group of devices on which to run the task. Upon selecting a device or group, the page will update.
3. Command Script to Run — Choose either:

    a) Cisco IOS Remove Line from ACL by ACL ID

    - Id of ACL to delete line from — Enter the ACL ID that you want to remove a line from. If you have selected a group of devices, this will remove a line from each device ACL that matches this ACL ID.
    - ACL line to delete — Enter the ACL line exactly as it appears on the device. Keep in mind that some ACL lines have multiple space characters, for example: `access-list 139` and `deny ip host 192.168.139.2 any` contains three spaces between "deny" and "ip."
    - Update Scripts — Click when you have completed the above variables.
    - Parameters — Optional parameters.
    - Script — This is the actual script that will update the ACL. The option to edit this script before execution makes this feature very flexible.

    b) Cisco IOS Remove Line from ACL by Handle

    - ACL Handle — Enter the ACL Handle that you want to delete a line from. If you selected a group of devices, this will delete a line from each device that contains an ACL that matches this ACL Handle.
    - ACL line to delete (without 'access-list {id}') — Enter the ACL line that you want to delete without any "access-list ACLID." The script will place this if necessary.
    - Update Scripts — Click this when you have completed the above variables.
    - Parameters — Optional parameters.
    - Script — This is the actual script that will update the ACL. The option to edit this script before execution makes this feature very flexible.

Commenting ACLs and Creating ACL Handles

NA integrates an in-line commenting feature with ACL comments. This allows the comments for an ACL to be included in the configuration and for changes in the configuration comments to get included and reapplied to the ACL.

On devices that support in-line commenting, the ACLNAME: text following the double-comment character sequence that identifies a NA in-line comment indicates the ACL Handle. On devices that do not support in-line commenting, the ability to move ACL comments to and from the configuration is not available. However, ACL comments and handles will continue to be maintained within the ACL.

To enter comments:

1. On the menu bar under Devices, click Inventory.
2. On the Inventory page, select the device that has ACL parsing enabled. The Device Details page opens.
3. From the View drop-down menu, select Device Detail and click ACLs. The Device ACLs page opens.
4. Click the View ACL option. The View ACL page opens. Refer to “View ACL Page Fields” on page 687.
5. Click the Edit Comments option. The Edit ACL page opens.
6. Enter comments in the Comments field.
7. Edit the ACL Handle.
8. Click Save.

For devices that support NA in-line commenting, changing the comments in the configuration will be reflected in the ACL comments.

Creating ACL Templates

In addition to directly creating scripts based on existing ACLs, you can use ACLs to form the basis for ACL command script templates. ACL templates can also be created for editing and applying ACLs.

1. On the menu bar under Devices, click Inventory.
2. On the Inventory page, select the device that has ACL parsing enabled. The Device Details page opens.
3. From the View drop-down menu, select Device Detail and click ACLs. The Device ACLs page opens.
4. Click the View ACL option in the Actions column. The View ACL page opens.
5. Click the New ACL Template link under the ACL Script. The New Command Script page opens. Refer to "New Command Script Page Fields" on page 584. The following fields in the New Command Script page are automatically populated:
   - Script Type — Displays the ACL script template type being created, including: ACL Creation Script, Edit ACL Script, or Apply ACL Script.
   - Mode — displays the correct script mode to run the ACL script on the device.
   - Script — Displays a copy of the existing ACL application scripting.

   Note: You can use the reserved variable "$tc_aclid_for_handle$" in your script when you need an ACL ID. When you run the script, you are prompted for the ACL handle. When the script is actually run on the device, each instance of this variable in the script will be replaced by the ACL ID on the device whose handle matches what you provided.

6. Enter a name for your new ACL creation script.
7. Edit the script. Refer to "Running Command Scripts" on page 689 for information.
8. Be sure to click Save Script when you are finished. When the script is saved successfully, the Script Search Results (Command Scripts) page opens. The script you added appears in the list and is highlighted. Keep in mind that a script does not run until you schedule it as a task.
9. Select the Run action.
10. Specify the Hostname or IP address of one device that is capable of running the script.
11. Enter the ACL ID.
12. Save the task. When the task is complete, the new ACL is displayed on the View ACL Page. Refer to "Device ACLs Page Fields" on page 685.

Editing ACLs

To edit an ACL:

1. On the menu bar under Devices, click Inventory.
2. On the Inventory page, select the device that has ACL parsing enabled. The Device Details page opens.
3. From the View drop-down menu, select Device Detail and click ACLs. The Device ACLs page opens.
4. Click the Edit ACL option for the ACL you want to edit. The Run Command Script page opens. Refer to "Creating ACLs" on page 690 for information.

When you click the Edit ACL link, the following fields in the Run Command Script task are automatically populated:

- Command Script to Run — Displays the type of script (Edit ACL) and the source ACL.
- Limit to script types — Displays the type of script (Edit ACL Script).
- Mode — Displays the correct script mode for editing an ACL on the device.
- Script — Displays the device-specific commands to run. Be sure to check this thoroughly and make any necessary changes.

If you want to deploy the edited ACL to several devices, select the device group to which you want to deploy ACL. Refer to "Run Command Script Task Page Fields" on page 306 for information.

Note: You should not run ACL scripts line-by-line. ACL scripts can result in lost connectivity when run line-by-line.

Deleting ACLs

One of the more time-consuming tasks in ACL management is removing older, unused ACLs from devices so that they do not interfere with newer applications and ACLs. When deleting ACLs for a single device, the ACLs on that device are listed. When deleting ACLs for a group of devices, all ACL handles on all devices in the group are listed, and the deletion of ACLs is by handle, not by ACL ID.

To delete ACLs, from the Devices menu, select Device Tasks and click Delete ALCs. The New Task - Delete ACLs page opens. Refer to “Delete ACLs Task Page” on page 698.

When you delete an ACL from a device configuration, the ACL no longer appears in the list of managed ACLs. Although the history of the ACL is still searchable using the Search For ACL option, the ACL history is not displayed when viewing device specific ACLs. There is no tracking of deleted ACLs from a device specific interface. To rollback the configuration of a deleted ACL, search for that ACL and then re-deploy it.

Keep in mind that ACLs that have no applications are deleted. However, ACLs with applications are not deleted. By default, NA will not delete ACLs if they have an application script. An option is provided that forces the deletion of ACLs even if they have applications. If this is checked, all ACLs selected will be deleted.

Note: NA does not guarantee that it will locate all applications of an ACL in the device's configuration. It is possible that an ACL has no application script, but is actually in use somewhere on the device. In such cases, the Delete ACLs task will attempt to delete the ACL (since it knows of no applications), resulting in unexpected device behavior.

Delete ACLs Task Page

The Delete ACLs task enables you to delete ACLs. To delete ACLs, from the Devices menu, select Device Tasks and click Delete ALCs. The Delete ACLs page opens. When you are finished click the Save Task button.

Field	Description/Action
Task Name	Displays Delete ACLs. You can enter a different task name if applicable.
Applies to	Select one the following options: • Device / Group — Enter an IP Address, Hostname, or Device Group name on which to run the task against or click the magnifying glass icon. For information on how to use the Device Selector, refer to "Device Selector" on page 144. • CSV File — Enter the name or browse for the CSV file containing a list of devices. The CSV file must provide a method to identify the device associated with each of the rows (IP address and Hostname) in the CSV file. If you click the Task CSV Template link, you can download a sample CSV file.
Start Date	You can select the following options: • Start As Soon As Possible — If selected, the default, the multiple task job will start as soon as possible. • Start At — If selected, you can click the calendar icon to open the calendar where you can select the date and time to start the multiple task job.
Priority	Displays the task's priority. There are five task priority levels, 1 through 5. 1 is the highest task priority level. Refer to "Scheduling Tasks" on page 280 for more information.
Comments	Add any comments about the multiple task job.
Task Options	
Session Log	Check the "Store complete device session log" box to store a debugging log. This is useful when debugging a failed snapshot, however large amounts of data can be stored.
Force Save	The device configuration update setting. This setting applies to only those devices that support a startup configuration. The default value of this setting is configurable per task type. • If NA should overwrite the startup configuration with the current running configuration at the completion of this task, select the Force Save check box. • If NA should not change the startup configuration, clear the Force Save check box. (**Note**: This setting is new in NA 9.20. It overrides all other approaches to determining whether to update the device startup configuration.)
ACLs to delete	You can select the following options: • Show ACLs without applications — Displays only ACLs without known applications (the default). • Show all ACLs — If selected, all ACLs, including the ACL IDs, with handles in parentheses, are displayed. You can select any number of ACLs from the list. (Note: If you are running this task against a group of devices, the list contains all ACL handles found on all devices in the group. There is no option to filter the list by ACLs without applications.)

Field	Description/Action
Delete ACLs even with applications check box	If checked, selected ACLs are deleted even if they have known applications.
Estimated Duration	Enter the amount of time for which you want to reserve the device or device groups that this task is to run against. The default is 60 minutes.
Device Credentials Options Device credentials options are displayed depending on the Allows Standard Device Credentials, Allow Per-Task Device Credentials, and/or the Allow User AAA Credentials options configured on the Server page under Administrative Settings. If Allow Per-Task Device Credentials is enabled, you are prompted to enter the appropriate credentials. In addition, if more than one Device Credentials option is enabled, you are prompted to select which option to use when running the task. If only one Device Credentials option is enabled, it is used automatically and you are not prompted. (Refer to "Device Access Page Fields" on page 47 for information on enabling Device Credentials.)	
Device Credentials	Depending on the Device Credentials options enabled on the Device Access page under Administrative Settings, you can select one or more of the following options: • Use standard device-specific credentials and network-wide password rules (the default). • Use specific task credentials. You are prompted to enter a Username, Password, Confirm Password, Enable Password, Confirm Enable Password, SNMP Read-Only Community String, and a SNMP Read/Write Community String. • Use task owner's AAA credentials. The task owner must have valid AAA credentials defined. (**Note**: Standard password rules and device-specific passwords are used. However, the task owner's AAA username and password are applied.)
Pre-Task / Post-Task Snapshot Options Snapshot options only appear if the system is configured to enable user overrides on the Configuration Mgmt Page under Administrative Settings. (Refer to "Configuration Mgmt Page Fields" on page 38 for information.)	
Pre-Task Snapshot	Select one of the following options: • None • As part of task (the default)
Post-Task Snapshot	Select one of the following options: • None • As part of task (the default) • Scheduled as a separate task
Approval Options Approval options are only displayed if the task is part of a Workflow Approval Rule.	
Request Approval	Checked by default if the task needs approval before it can run. To change the date by which the task must be approved, click the calendar icon next to the date to open the calendar and select a date and time. You can also select a task priority. Keep in mind that you can add different priority values, such as Urgent and Normal, when configuring Workflows. The NA Scheduler does not look at the values. They are basically a visual queue for you to determine which tasks need approval in a timely manner.
Override Approval	If the task allows override, select this option to override the approval process.

Field	Description/Action
Save as Draft	If checked, you can save the task as a draft and return to it later. The task will not run in Draft mode.
Scheduling Options	
Retry Count	If the task fails, NA will try the task again this many times, allowing for the Retry Interval between retries. Select one of the following options: • No Retry (the default) • Once • Twice • Three Times
Retry Interval	Enter the number of minutes to wait before trying again. The default is five minutes.
Recurring Options	The task will begin on the date/time specified above, then recur per the following. Select one of the following options: • Once Only — The task occurs only once on the specified date/time (the default). • Periodically — Specify a Repeat Interval in minutes. • Daily — The task occurs each day at the specified time. • Weekly — Select one or more days of the week. The task occurs on these days at the specified time. • Monthly — Select the day of the month the task occurs once each month on this day at the specified time.
Range of Recurrence	If you select any of the recurring options, with the exception Once Only, you can specify a range of recurrence, including: • No End Date (the default) • End after < > occurrences — Enter the number of occurrences. • End by — Click the calendar icon and select a date and time.

Chapter 21: Troubleshooting

Use the following table to quickly locate information.

Topic	Refer to:
Driver Discovery Failed	"Driver Discovery Failed" on page 702
Device Snapshot Failed	"Device Snapshot Failed" on page 703
No Real-Time Change Detection via Syslog	"No Real-Time Change Detection Via Syslog" on page 704
Session Logs	"Session Logs" on page 705
SWIM Error Messages	"SWIM Error Messages" on page 706

For information on Logging, refer to "Logging" on page 98. For information on sending Troubleshooting information to Customer Support, refer to "Send Troubleshooting Page Fields" on page 31.

Driver Discovery Failed

If you cannot discover a driver for a device:

1. Make sure that the device you are trying to discover is a supported device model and OS version. Refer to the Driver Release Service (DRS) documentation for detailed information on supported devices. The DRS is an automated driver release and delivery system. If the device is not supported, contact Customer Support. If the device is supported, go to Step 2.
2. Telnet and/or SSH to the device from the NA server. An easy way to verify that NA can Telnet or SSH to a device is to click the Telnet or SSH link for the device on the Device List page. Refer to "Inventory Page Fields" on page 188 for information. NA automatically attempts to login to the device. If you cannot login to the device, this could be caused by incorrect access lists on the device, incorrect password information, or network connectivity issues. Contact Customer Support. If you can Telnet and/or SSH to the device, but the Discover Driver task still fails, go to Step 3.
3. Check to see if you have read-only SNMP enabled on the device. If read-only SNMP is enabled, using this OID, try to contact to the device via read-only SNMP from the NA server. Make sure you use the community string you configured for the device within NA. If you do not want to enable read-only SNMP, you can manually select the driver from the driver drop-down list when you add or edit devices. Refer to "Editing Device Configuration Data" on page 180 for information. Once you have enabled read-only SNMP, login to NA, select the device you are trying to add, and click Edit Device. Update the device with the correct read-only SNMP community string and click Discover Driver. If the Discover driver task still fails, go to Step 4.
4. Login to NA. On the menu bar, select Admin and click the Troubleshooting option. The Troubleshooting page opens. In the list box, select device/session/log and device/driver/discovery. Set the level to Trace (most message). Click Submit. Click the device you are attempting to discover and then click Discover Driver. Once the Discover Driver task fails, on the menu bar select Admin and click Troubleshooting. Click Send Troubleshooting Information. In the comments section, specify what is failing and the device model and OS version. For information on Logging, refer to "Logging" on page 98.

Device Snapshot Failed

If a device snapshot failed:

1. Make sure the device you are trying to snapshot is a supported device model and OS version for NA. Refer to the Driver Release Service (DRS) documentation for detailed information on supported devices. The DRS is an automated driver release and delivery system. If the device is not supported, contact Customer Support. If the device is supported, go to Step 2.
2. Make sure that there is a device driver assigned to the device. On the Device List page, click the problem device. Refer to "View Menu Options" on page 203 for information. Scroll down to the Driver Name field and check if it has a value. If there is no driver, contact Customer Support. If there is a driver, click the Discover Driver link. If the Snapshot task still fails, go to Step 3.
3. Telnet and/or SSH to the device from the NA server. An easy way to verify that NA can Telnet or SSH to a device is to click the Telnet or SSH link for the device on the Device List page. Refer to "Inventory Page Fields" on page 188 for information. If you cannot login to the device, this could be caused by incorrect access lists on the device, incorrect password information, or network connectivity issues. Contact Customer Support. If you can Telnet and/or SSH to the device, but the Discover driver task fails, go to Step 4.
4. Check to see if you have read-only SNMP enabled on the device. If read-only SNMP is enabled on the device, using this OID, try to contact the device via read-only SNMP from the NA server. Make sure you use the community string you configured for the device within NA. If you do not want to enable read-only SNMP, you can manually select the driver from the driver drop-down list when you add or edit devices. Refer to "Editing Device Configuration Data" on page 180 for information. Once you have enabled read-only SNMP, login to NA, select the device you are trying to add, and click Edit Device. Update the device with the correct read-only SNMP community string and click Snapshot. If the Snapshot task still fails, call Customer Support.

No Real-Time Change Detection Via Syslog

If there is no real-time change detection via Syslog:

1. Make sure that the device you are trying to snapshot is a supported device model and OS Version for NA. Refer to the Driver Release Service (DRS) documentation for detailed information on supported devices. The DRS is an automated driver release and delivery system. If the device is not supported, contact Customer Support. If the device is supported, go to Step 2.
2. Make sure the Syslog settings are configured correctly so that Syslog messages are reaching the NA server. Initiate an event that will trigger a Syslog change message to be sent to NA.
3. Make sure that the device/OS combination supports real-time change detection via Syslog. Refer to the Driver Release Service (DRS) documentation for detailed information on supported devices. The DRS is an automated driver release and delivery system. If possible, verify on the vendor’s website that Syslog notification of change is available in this device and OS. If the device does not support real-time change detection via Syslog, go to Step 4.
4. There is another method by which NA provides real-time change detection: AAA logging. Check to see if you have AAA change detection enabled. Refer to “Configuration Mgmt Page Fields” on page 38 for information. If you are using AAA, make sure that the device supports real-time change detection via AAA.

Session Logs

The difficult part of any automation task is not the automation itself, but trying to determine the cause of failure if an automation task fails. NA provides detailed troubleshooting capabilities to help you quickly identify reasons for failure and resolve them.

NA provides a detailed device session log from any device task. As a result, you can see what NA is sending to the device and how the device is responding.

1. Log into NA.
2. On the main menu bar under Devices and select New Device Task and click Run Command Script. The New Task - Run Command Script page opens.
3. In the Applies to field, enter a device hostname or IP address on which you are allowed to make configuration changes.
4. Under Task Options — Session Log, check the “Store complete device session log” box.
5. Under Task Options — Command Script to Run, select the command script you want to run from the drop down menu.
6. Specify the mode to run in. For example, if this is an IOS device, select Cisco IOS Configuration.
7. Enter the commands you want to send to the device.
8. Click the Save Task button.

As the task runs, you will see the output of the NA <-> device interaction. You should be able to determine:

- What NA sent to the device.
- What NA expected to receive from the device.
- What NA actually received from the device.

SWIM Error Messages

Message-ID	Error Message	Probable Cause	Possible Action
SWIM0019	Could not perform Image recommendation for the selected device(s) because of insufficient data.	Could not fetch Image information from the database.	Make sure inventory collection has succeeded. For the selected device, run the OS Analysis task and launch Software Upgrade Recommendation.
SWIM0089	Could not perform Image Import from Cisco.com on the selected device(s).	Add Image from Cisco.com not supported for the device. This is because Cisco.com could not find the device platform in the supported list	None
SWIM0092	Error while fetching inventory information for the device.	Check whether you have privileges to use this device and whether inventory has complete data for this device.	For the selected device, run the OS Analysis task.
SWIM0093	Could not get Image information from Cisco.com	Could not connect to Cisco.com from CWNCM Server either because of incorrect Cisco.com credentials or missing proxy configuration.	Check whether Cisco.com credentials are correct. If they are correct, check whether the proxy server is configured with right proxy credentials. To configure the proxy, go to CWNCM home page > click on Change Password > Select ìCisco.com Proxy for Credential Type > Enter user name and password.
SWIM0125	An unexpected error has occurred. Contact Cisco support and attach the SWIMNG_ server.log file.	None	Contact Cisco Technical Assistance Center (TAC) with the log available under: Windows: <CWNCM installed folder>\server\ext\swim\log\SWIMNG_server.log Solaris & Linux: <CWNCM installed directory>/server/ext/swim/log/SWIMNG_ server.log
SWIM0126	An unexpected error has occurred. Contact Cisco support and attach the SWIMNG_ server.log file.	None	Contact Cisco Technical Assistance Center (TAC) with the log available under: Windows: <CWNCM installed folder>\server\ext\swim\log\SWIMNG_server.log Solaris & Linux: <CWNCM installed directory>/server/ext/swim/log/SWIMNG_ server.log
SWIM0155	User is not authorized to download crypto image from Cisco.com	User is not authorized to download crypto image from Cisco.com.	Go o Cisco.com and sign the crypto agreement.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM0156	No response stream was obtained for the download request.	No response stream was obtained for the download request.	Please try it again later or directly download the image from Cisco.com website then add it into system.
SWIM1003	SNMP Agent does not support the required instrumentation to get information about the Flash File system.	The SNMP Agent on the device does not support CISCO-FLASH-MIB/OLD-CISCO-FLASH-MIB.	Check for any known bugs related to these MIBs for the image version running on the device.
SWIM1004	Cannot get details about the Flash File system on the device.	There may be a faulty implementation of the MIB on the device.	Check Cisco.com for any known issues for the running image version.
SWIM1005	Flash Device or Partition does not exist on the device.	Either the Inventory data on the device is stale, or the selected Flash Device or Partition is invalid.	For the selected device run the OS Analysis task and launch Software Upgrade Recommendation.
SWIM1006	Flash Partition does not exist on the device.	Either the Inventory data on the device is stale, or the selected Flash Partition is invalid.	For the selected device run the OS Analysis task and launch Software Upgrade Recommendation.
SWIM1027	Error while fetching inventory information.	The data required for the selected task is either incomplete or missing in Inventory.	For the selected device run the OS Analysis task and launch Software Upgrade Recommendation.
SWIM1029	Cannot get the required inventory information for the device.	Either there was no inventory collection for the device or the device is not responding.	For the selected device run the OS Analysis task and launch Software Upgrade Recommendation.
SWIM1030	This is a Run From Flash (RFF) device, but the application cannot find the running image on the Flash.	Either the inventory has not been updated or the Flash file is deleted from the Flash.	For the selected device run the OS Analysis task and launch Software Upgrade Recommendation.
SWIM1031	No Candidate Images found for the running software.	Either Cisco.com is not included in the My Preferences or there are no applicable images in the software repository or Cisco.com	Check Admin > Users > Select your user name and click on the 'Permissions' associated with it > My Preferences or add images to software repository. Re-launch Software Upgrade Recommendation.
SWIM1032	Images obtained for Recommendation do not meet the hardware and software requirements of the selected device.	Either the Candidate Images were filtered based on the selected My Preferences or they did not meet the Flash/RAM/BootROM needed to run on the device.	Check Admin > Users > Select your user name and click on the 'Permissions' associated with it > My Preferences. Or add images to software repository. Re-launch Software Upgrade Recommendation.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1033	Cannot find the Best-fit image for the device by applying compatibility checks.	Either the Candidate Images were filtered based on the selected My Preferences or they did not meet the Flash/RAM/BootROM needed to run on the device.	Check Admin > Users > Select your user name and click on the 'Permissions' associated with it > My Preferences or add images to software repository. Re-launch Software Upgrade Recommendation.
SWIM1034	No applicable images found for the device from the configured image sources.	Either Cisco.com is not included in the My Preferences or there are no applicable images in the software repository or Cisco.com	Check Admin > Users > Select your user name and click on the 'Permissions' associated with it > My Preferences or add images to software repository. Re-launch Software Upgrade Recommendation.
SWIM1035	Error while performing Recommendation option. Runtime error encountered while filtering images caused by a problem with a running image on the device.	None	Retry the operation. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: Windows: <CWNCM installed folder>\server\ext\swim\log\SWIMNG_server.log Solaris & Linux: <CWNCM installed directory>/server/ext/swim/log/SWIMNG_server.log
SWIM1036	Runtime error while performing Recommendation.	None	Retry the operation. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: Windows: <CWNCM installed folder>\server\ext\swim\log\SWIMNG_server.log Solaris & Linux: <CWNCM installed directory>/server/ext/swim/log/SWIMNG_server.log
SWIM1037	Error while fetching Flash Partition information.	Either the Flash information cannot be got from Inventory or there is a problem with the running image on the device.	For the selected device run the OS Analysis task and launch Software Upgrade Recommendation. If the problem persists, check Cisco.com for any known issues on the running image version.
SWIM1038	No Read-Write Partition found on the device.	None	Install a flash device with a read-write partition and update the inventory.
SWIM1039	No Storage Recommendation is made for the device.	The selected device may not have sufficient free size partition to copy the image.	Check whether the selected device has the sufficient free size partition to copy the image.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1040	Cannot get the Flash information for the device.	Either the Flash information cannot be got from Inventory or there is a problem with the running image on the device.	For the selected device run the OS Analysis task and launch Software Upgrade Recommendation. If the problem persists, check Cisco.com for any known issues on the running image version.
SWIM1041	This device upgrade requires opening an SSH/ Telnet connection to the device.	Enable password is not configured correctly for device.	Make sure that the appropriate SSH/ Telnet passwords are configured correctly for device.
SWIM1042	The amount of Bootflash on the device may not be enough to run the selected image.	The amount of Bootflash on the device may not be enough to run the selected image.	None
SWIM1043	Runtime error while performing Bootloader image verification.	Selected image version may not be in the standard version format.	Retry the operation. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: Windows: <CWNCM installed folder>\server\ext\swim\log\SWIMNG_server.log Solaris & Linux: <CWNCM installed directory>/server/ext/swim/log/SWIMNG_ server.log
SWIM1044	Bootflash partition will be erased before copying new image.	Selected Bootloader image does not fit in available space on Bootflash.	Select a different Bootloader image if available.
SWIM1046	Selected software does not fit in selected Flash partition.	Selected software image does not fit in the available space on Bootflash.	Select a different Flash partition for upgrading.
SWIM1048	The system software that is active on the device, cannot run the selected image.	The system software that is active on the device, is not compatible with the selected image.	Select a different image that can be upgraded with the current system software or upgrade the system software to Software Version.
SWIM1049	The selected image requires Flash to be erased during image upgrade.	None	Check whether you have performed the necessary backup.
SWIM1050	Read-Write SNMP community string is not available for the device.	The Read-Write SNMP community string is not available for the device.	Add Read-Write community string for the device.
SWIM1051	Credential information cannot be obtained for the device.	Either the device is not managed in the CWNCM server or the device credentials are not correct or the device access privileges are insufficient.	None

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1052	Enable password is not configured for the device.	For the Run From Flash (RFF) partition software upgrades, the Enable password must be configured.	Configure the Enable password for the device.
SWIM1053	Selected MICA Image is the same as the running image on the device.	The software version of the image is the latest on the device.	None
SWIM1054	Error while checking the Telnet credential of the device.	None	Make sure that the Telnet credentials for the device are correct.
SWIM1055	Selected Flash partition is Read-Only.	Either the Flash partition is not write-enabled or the Read-Write partition does not exist.	Check whether the Read-Write partition exists. Set the Flash partition to be write-enabled.
SWIM1056	The method to update the software on the selected storage device is unknown.	None	Select a different Flash partition, if available.
SWIM1057	The device will be put into Rxboot mode for the image upgrade.	None	Select a different Flash device for the system software, if available.
SWIM1058	The selected software version has some known issues in the Flash MIB options that make this application unable to perform software upgrades on the device.	None	Upgrade the device manually or select a later software version, if available.
SWIM1059	Ensure Dial Shelf runs a compatible software image with the newly loaded Router Shelf software image.	The Router shelf software image is not compatible with the Dial Shelf software image.	See the Release Notes for the Router Shelf software image to make sure the current Dial Shelf software is compatible. If not, upgrade the Dial Shelf software.
SWIM1060	Cannot obtain the file size of the selected image.	The selected image may have been removed from Cisco.com.	Select another image for upgrading.
SWIM1062	Selected image is already running on the device.	None	Verify that this is the image you want to upgrade for the device.
SWIM1063	Minimum RAM requirement of the selected image cannot be determined.	RAM available on the device may not be enough to activate this image.	None
SWIM1064	RAM available on the device may not be large enough to activate the selected image.	RAM available on the device may not be large enough to activate the selected image.	Select a different image or upgrade the RAM on the device.
SWIM1065	RAM available on the device may not be enough to activate the selected image.	RAM available on the device may not be large enough to activate the selected image.	Select a different image for upgrading.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1067	Runtime error while performing verification of the selected image.	None	Select a different image for upgrading. If not fixed, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: Windows: <CWNCM installed folder> \server\ext\swim\ log\SWIMNG_server.log Solaris & Linux: <CWNCM installed directory>/server/ ext/swim/log/SWIMNG_ server.log
SWIM1068	Selected image does not have the minimum system software version required for the upgrade.	Selected image does not have the minimum system software version required for the upgrade.	Select a different image with a version higher than 11.0.
SWIM1069	Feature subset of the selected image is a subset or equal to running software feature set. Select a different image.	Feature subset of the selected image is a subset or equal to running software feature set.	Select a different image.
SWIM1070	Feature subset of the running image cannot be determined. Select a different image.	Feature subset of the selected image is a subset or equal to running software feature set.	Select a different image.
SWIM1075	Cannot find an image that is newer and can fit on the Bootflash.	None	Add Bootloader images to the Software Repository, with version greater than the running image version and that can fit into the Bootflash.
SWIM1076	Cannot find a Read-Write Boot partition on the device.	Read-Write Boot partition is not available on the device.	Insert a read-write Bootflash on the device and update the inventory.
SWIM1077	Cannot find a Bootflash partition for the Bootloader image.	Bootflash partition is not available for the Bootloader image.	Insert a read-write Bootflash on the device and update the inventory.
SWIM1079	Image version cannot be compared.	The image formats of both the images may not be compatible for comparison.	Check the format of the version. Select a different image for upgrading.
SWIM1082	Runtime error while comparing Modem Image.	Either a wrong modem image is selected for comparison or the modem image formats is not compatible.	Select a different Modem Image for upgrading. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: Windows: <CWNCM installed folder>\server\ext\swim\log\SWIMNG _server.log Solaris & Linux: <CWNCM installed directory>/server/ ext/swim/log/SWIMNG_ server.log

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1083	Cannot find an image that is newer and fits in the Flash.	None	Add another image into software repository and retry the operation.
SWIM1084	Cannot find a Minimum Flash Requirement for the device.	The Flash space available on the device may not be sufficient for the selected image.	Check whether the image fits on the device.
SWIM1085	The MinFlash Attribute is unknown for the selected image.	The selected image does not fit on the selected partition.	Check whether the image fits on the selected partition or select a different image.
SWIM1087	Cannot get the device representation.	Unable to retrieve the device details from the inventory.	Capture the logs and contact the Cisco Technical Assistance Center (TAC). The debug logs available at this location: Windows: <CWNCM installed folder>\server\ext\swim\log\SWIMNG_ server.log Solaris & Linux: <CWNCM installed directory>/server/ext/swim/log/SWIMNG_server.log
SWIM1092	Selected image does not have the minimum system software version required for system upgrade.	None	Select an image that has a higher version than the minimum supported version. See the documentation for the Compatibility Matrix for Cisco IOS software.
SWIM1093	Cannot get Chassis Information from the inventory.	None	For the selected device run the OS Analysis task and launch Software Upgrade Recommendation.
SWIM1094	SNMP-V3 parameters is incorrect or not available for the device.	This could have been caused by any of the following: • The SNMP-V3 password is wrongly configured • The SNMP-V3 algorithm is wrongly configured • The SNMP-V3 engine ID is not configured for the device.	Check whether the SNMP-V3 password, SNMP-V3 algorithm, and SNMP-V3 engine ID is configured for the device.
SWIM1095	Error while checking the SNMP-V3 user name in the device context.	None	Update the SNMP-V3 credentials for the device. For the selected device run the OS Analysis task and launch Software Upgrade Recommendation.
SWIM1097	Selected Bootloader image is a lower version than the version of the Bootloader running on the device.	The Bootloader image version running on the device is the latest.	Check whether the higher version is available for upgrading.
SWIM1098	The selected image is lower than the running image on the device.	The image version running on the device is the latest.	Select a higher image for device software upgrade. (no change needed)

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1099	Image Upgrade procedure may revert to the SSH/ Telnet-based approach, based on the MIB instrumentation on the running image.	The SSH/Telnet passwords may not be configured for the device.	Make sure that appropriate SSH/ Telnet passwords are configured for the device.
SWIM1100	Cannot find SNMP-V2 Read-Write Community String for the device.	The SNMP-V2 credentials may not be correctly configured for the device.	Check whether the SNMP-V2 credentials are configured correctly for the device.
SWIM1101	This Device Upgrade requires opening an SSH/ Telnet connection to the device.	Enable password for the device is not configured for the device.	Make sure that appropriate SSH/ Telnet passwords are configured correctly for the device.
SWIM1102	This Device Upgrade requires opening a SSH/ Telnet connection to the device.	There was an error while checking the credentials of the device.	Make sure that appropriate SSH/ Telnet passwords are configured correctly for the device.
SWIM1103	Selected image may not be compatible to the device.	Image belongs to the same device family as the running image on the device. However, it is identified as non-compatible.	Check the Cisco.com documentation whether any caveats are identified for the selected image.
SWIM1105	Image status for the selected image cannot be determined.	The selected image might be in the Deferred status.	Ensure that the image is not in the Deferred status. See the relevant documentation on Cisco.com before upgrading the images.
SWIM1106	Image selected for upgrade is compressed in .tar format. Flash will be overwritten while upgrading the image.	None	Ensure that necessary backup jobs are completed before upgrading.
SWIM1107	This option requires *devicename* data in the inventory.	The required device information is not available in the inventory.	For the selected device run the OS Analysis task and launch Software Upgrade Recommendation.
			Continued on next page
SWIM1109	Image status for the selected image is either Deferred or Not Supported.	Image status for the selected image is either Deferred or Not Supported.	Ensure that the image is supported by CWNCM application. Check the documentation on Cisco.com before upgrading the image.
SWIM1111	The available free space is not enough for upgrading this type of image.	Insufficient space for image upgrade.	Select a different image or free up some space. Update the inventory and retry the job.
SWIM1112	This module can be upgraded if managed independently.	This module can be upgraded only if it is managed as a separate device.	Assign an independent IP Address to this module. Manage it as a separate device and select that device to upgrade this module.
SWIM1116	Read-Write SNMP community string cannot be fetched from the Device Context.	The Read-Write community string is not available for the device.	Add the Read-Write community string for the device.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1118	Selected image has a lower version than the version of the running image.	The selected image has a lower version than the version of the running image.	None
SWIM1119	Telnet credentials are not present for this device. There was an error while checking the credentials for the device.	The SSH/Telnet passwords are not configured correctly for the device.	Ensure that appropriate SSH/Telnet passwords are configured correctly for the device.
SWIM1120	Cannot obtain the sysObjectID of the device.	None	For the selected device run the OS Analysis task. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: Windows: <CWNCM installed folder>\server\ext\swim\log\SWIMNG_server.log Solaris & Linux: <CWNCM installed directory>/server/ext/swim/log/SWIMNG_ server.log
SWIM1122	Runtime error found during verification.	None	Retry the operation. If the problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: Windows: <CWNCM installed folder>\server\ext\swim\log\SWIMNG_server.log Solaris & Linux: <CWNCM installed directory>/server/ext/swim/log/SWIMNG_server.log
SWIM1123	Telnet username not present for this device.	None	Check whether the primary username is configured for the device.
SWIM1139	Select any available boot flash partition, for bootldr upgrade. We recommend that you use boot flash for bootldr upgrade.	This happens when the user has selected a Bootloader image for Distribution and a storage location other than bootflash.	Select any available boot flash partition for bootldr upgrade.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1162	Error when recommending image for the device.	Image software Recommendations are based on device ROM, RAM and Flash which is collected in the inventory. If the device is having a faulty hardware (FLASH) then this will not be available in inventory.	Check the device for a faulty hardware or a bug in device software. For the selected device run the OS Analysis task and launch Software Upgrade Recommendation. If problem persists, send the debug logs to Cisco Technical Assistance Center (TAC). The debug logs are available at this location: Windows: <CWNCM installed folder>\server \ext\swim\log\SWIMNG_ server.log Solaris & Linux: <CWNCM installed directory>/server/ ext/swim/log/SWIMNG_ server.log
SWIM129	Selected image does not fit on the free Flash size on the device. Selected storage partition will be erased during the distribution.	Either: The boot loader image is selected for upgrade (and no system software image is selected along with it) or the storage location is not erased for the boot loader image to be copied.	Since the system software is not selected for upgrade, ensure that running system software is not in the selected storage partition. Back up the running system software and ensure that the device boots from the backed up image in case the job fails.
SWIM1501	Supervisor cannot be downgraded to an image version less than 4.1(1).	This happens when you try to distribute a CATOS image lesser than 4.1(1).	If you continue to downgrade, the device may lose its configuration. Use a higher version.
SWIM1525	Unknown package type.	None	The selected module is not supported.
SWIM1529	There is no module information available in the inventory for *devicename*.	There is no module information available in the inventory for *devicename*.	For the selected device run the OS Analysis task.
SWIM1530	Storage Recommendation is not supported for the Module *modulename*.	None	Storage recommendation is not supported for this module, may be because the module has reached end-of-sale or end-of-life.
SWIM1532	No read-write partition exists on the device to accommodate the selected image.	None	Create sufficient free space.
SWIM1542	Minimum supported version for Supervisor is 3.8.	None	Select a higher version of the image to upgrade.
SWIM1543	Selected image has the same or a lower version than the version of the running image.	The selected image has the same or a lower version than the version of the running image.	None
SWIM1546	The NVRAM size on the device may not be large enough to run the image.	The NVRAM size on the device may not be large enough to run the image.	Select a different image or upgrade the NVRAM on the device and retry the Upgrade option.

Message-ID	Error Message	Probable Cause	Possible Action
SWIM1547	Available NVRAM size on the selected image cannot be determined.	RAM size on this module may not be large enough to store this image.	Make sure the module has enough NVRAM to run the selected image. Else, select a different image or upgrade the RAM on the module.
SWIM1548	There are no software requirements found for the selected image.	None	Select a different image.
SWIM1549	Verify that the new software selected is compatible.	Software Management cannot determine the features in the ATM software.	Check the Release Notes for the new software to determine if all the features in the old software are available in the new software.
SWIM1554	The selected image cannot be used to upgrade the device.	The device does not have any module that can run the selected image.	Select a different image.
SWIM1560	Slot number corresponding to the module cannot be got from inventory.	None	For the selected device run the OS Analysis task and launch Software Upgrade Recommendation.
SWIM2001	Telnet error while connecting to the device. Cannot connect to device Device.	Invalid access information for the device.	Verify the username and the passwords for the device and then retry the task.
SWIM2002	Cannot get details about Flash File system on the device.	Either the Flash device is not available or the Flash information format has changed.	Check the Flash device and re-run the OS Analysis task.
SWIM3501	Cannot fetch device credentials for the selected device.	The credentials may not be configured correctly for the device.	Check whether the credentials are configured for the device.
SWIM3703	Selected image does not have the minimum system software version required for system upgrade.	None	Select a different Image with a version higher than 11.3(0).
SWIM5001	Cannot connect to the device *devicename* using protocol.	The device may not be reachable or there is invalid access information for the device.	Verify whether the device is reachable and the credentials are correct.
SWIM4800	The version running on the device is less than the minimum supported version.	None	Manually upgrade the device to the minimum supported version or higher.

Appendix A: Command Line Reference

To open a command window, in the Search tab on the left-hand side of the display, enter a device IP address or hostname and click the Connect button.

You can also open a command window from the Device Details page using the Connect menu. Within the command window, you can select the text that you want to copy and press the Return key. The highlighted text is placed into a copy buffer. You can then paste it into another application. Enter `exit` and close the window when you are finished.

Note: If you use the Telnet/SSH Proxy to connect directly to devices, you remain in the Telnet/SSH Proxy when you exit the device. Unless you enter `exit` again, you can enter CLI commands and connect to other devices.

To view Help for CLI commands, enter: `help` to see a list of all commands. Enter `help <command name>` to see detailed help on a specific command.

Note: The CLI is not case-sensitive. You can enter all commands and options in lowercase or uppercase.

CLI Help is available online using the following commands:

- At the CLI prompt, enter: `help`. You should see a list of nearly all the CLI commands in alphabetical order. For example, to see Help for the Import command, enter: import. (**Note**: There is no Help text for the help or the exit/quit commands.)
- To view help information for the Import command, for example, enter: `help import` The command help <command name> returns detailed information on that command, including the name, a synopsis, a description, and examples.
- When you are finished with the command line, enter: `exit`. Depending on the type of session you started, you may need to enter exit again and manually close the window.

Note: You can also enter the help command and just the first word of a command to return a list of all the commands that begin with the same first word.

The type conventions used in the CLI Help text have specific meanings. The following table lists the conventions and their meanings.

Convention	Meaning
>	A single right angle bracket indicates the command prompt where you enter your commands.
-	A dash precedes a command option.
< >	Angle brackets surround variable text that you must fill in, such as an IP address. Do not include the angle brackets.
[ ]	Square brackets delineate one or more optional elements.
|	A vertical pipe separates arguments within brackets. Include only one argument.

For a complete list of CLI commands, including syntax and examples, see the *NA CLI/API Command Reference*.

Appendix B: Command Permissions

Users must be explicitly granted the corresponding command permission for each action they want to perform, such as viewing a Web page or executing a command. A set of command permissions creates a command permission role. You can then apply the role to a user group to set the command permissions for that given user group. Refer to "New User Role Page Fields" on page 261 for more information.

Note: NA includes four types of permissions, including Command permissions, Modify Device permissions, Script permissions, and View Device permissions. Some Command permissions require one or more of the other permissions. Refer to "Command Permission Definitions" on page 721 for information.

Granting Command Permissions

To grant Command permissions:

1. On the menu bar under Admin, click User Roles & Permissions. The User Roles & Permissions page opens.
2. Click the New User Role link at the top of the page. The New User Role page opens. Refer to "Adding User Roles" on page 259 for information.

List of Commands

Add Device
Add Device Group
Add Event
Add SNMP Trap Config
Admin Settings
Administer Device Groups
Administer Users
Administer User Groups
Annotate Device Configuration
Authorize Concurrent Telnet/SSH Sessions
Backup Device Software
Batch Edit Device
Change Device Password
Check Configuration Policy Compliance
Configure Syslog
Connector Redirect
Data Pruning
Deduplication
Delete Access
Delete Device
Delete Device Configuration
Delete Diagnostics
Delete Driver
Delete Session
Delete Software Compliance
Delete Software Image
Delete Software Level
Delete System Event
Delete Task
Deploy Remote Agent
Deploy Software
Detect Network Devices
Discover Device Driver
Drivers
Edit ACL
Edit ACL Comments
Edit Config [Changed By] User
Edit Device
Edit Inactive Device
Edit Task
Edit User
Email Report
External Authentication Setup
Generate Summary Reports
Import Devices and Passwords
ListSysOIDs
List View
Manage ACL
Manage Command Script
Manage Configuration Policy
Manage Device Password Rule
Manage Diagnostic Script
Manage Event Rule
Manage Enhanced Customer Data
Manage Distributed System
Manage Gateways
Manage IP Address
Manage License
Manage Partition
Manage Software Compliance
Manage Software Levels
Manage Software Image
Manage System Report
Manage Template
Manage User
Manage User Group
Manage User Role
Manage View
Modify Device Configuration
Modify SecurID
Multi-Task Project
Override Workflow Approvals
Reload Device Task
Resolve FQDNs
Run Command Script
Run Diagnostic
Run External Application
Run ICMP Test
Set Highest Priority For Tasks
Synchronize Recurring Task
Take Snapshot
Telnet/SSH Client
Troubleshooting
Update Device Comments
Update Device Ticket
Workflow Setup
View ACL
View Command Script
View Configuration Policy Event
View Deployed Software
View Configuration Policy
View Device Configuration
View Device Diagnostic
View Device Information
View Diagnostic Script
View Driver
View Event Rule
View Full Device Configuration
View Script & Diagnostic Result
View SecurID
View Session
View Software Image Archive
View Task
View Template
View User Information
View Workflow Setup

Command Permission Definitions

Command Permission	Description
Activate/Deactivate Device	Enables you to activate or deactivate devices.
Add Device	Enables you to add devices to the NA system. This permission includes adding devices via the Add Device Wizard.
Add Device Group	Enables you to create device groups. To create a public device group, you must also be granted the Administer Device Groups permission.
Add Device To Group	Enables you to add devices to a device group. Devices must already exist in the NA database.
Add Event	Enables you to use the New Message option from the Edit menu.
Add SNMP Trap Config	Enables you to configure SNMP traps and run the “add SNMP trap config” CLI command (which in turn adds to the config option “snmp/traps/global”).
Admin Settings	Enables you to change Admin settings. Keep in mind that there are some Admin settings that require additional permissions, such as Workflow Setup and External Authentication Setup.
Administer Device Groups	Enables you to manage device groups, including adding, modifying, and removing parent and public groups.
Annotate Device Configuration	Enables you to annotate device configurations.
Authorize Concurrent Telnet/SSH Sessions	Enables you to override the prevention of multiple proxy connections to a device.
Backup Device Software	Enables you to run the Backup Device Software task.
Batch Edit Device	Enables you to modify multiple devices during a batch edit.
Change Device Password	Enables you to schedule a task to change a single device’s password. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device for which the command is executed.
Change Device Password (Group)	Enables you to schedule a task to change passwords for a device group. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device group for which the command is executed.
Check Configuration Policy Compliance	Enables you to run the Check Configuration Policy Compliance task. The Check Policy Compliance task enables you to determine if devices are in compliance with either configuration policies or software compliance policies.
Clear Device Reservation	Enables you to clear device reservation conflicts that appear on the Activity Calendar.

Command Permission	Description
Configure Syslog	Enables you to schedule a task to configure a device's Syslog settings. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device for which the command is executed.
Configure Syslog (Group)	Enables you to schedule a task to configure a group of devices' Syslog settings. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device group for which the command is executed.
Connector Redirect	Redirects URL actions for NNM 7.x and NNM 8.x. Connector Redirect looks up the device ID from the IP address provided by NNM. In addition, Connector Redirect can forward device information, such as configuration history.
Data Pruning Task	Enables you to schedule the Data Pruning task for a single device. Data pruning removes obsolete files, diagnostics, events, and tasks.
Data Pruning Task (Group)	Enables you to schedule the Data Pruning task for a group of devices. Data pruning removes obsolete files, diagnostics, events, and tasks.
Deduplication	Enables you to remove or deactivate a single device, such that the device's interfaces only occur once within the NA database.
Deduplication (Group)	Enables you to remove or deactivate a group of devices, such that the devices' interfaces only occur once within the NA database.
Delete Access	Enables you to delete a device's access log.
Delete Device	Enables you to permanently delete a device from the NA database.
Delete Device Configuration	Enables you to remove device configurations.
Delete Device Group	Enables you to delete device groups.
Delete Diagnostics	Enables you to delete the diagnostic data captured by the task. Keep in mind that logs record how the diagnostic data was captured.
Delete Driver	Enables you to clear the assigned driver to a device.
Delete Event Rule	Enables you to delete Event Notification & Response rules.
Delete Session	Enables you to delete Telnet/SSH session records.
Delete Software Compliance	Enables you to delete software compliance records.
Delete Software Image	Enables you to delete software images from the NA software repository.
Delete Software Level	Enables you to delete a configured software level. NA has the ability to define software levels, essentially a regex to match against software versions. You can assign a software level to that regex. Any device with a software version that matches the regex is considered at that level.
Delete System Event	Enables you to delete system events.
Delete Task	Enables you to delete tasks.

Command Permission	Description
Deploy Remote Agent	Enables you to deploy the NA Remote Agent. The NA Remote Agent includes a process that handles SNMP and coordinates with the NA Management Engine on the NA Core, a Syslog process that handles Syslog notifications from local devices, and a TFTP process that enables TFTP access to local devices. (For information, see the *NA Satellite Guide*.)
Deploy Software	Enables you to schedule a task that deploys device software to a single device. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device for which the command is executed.
Deploy Software (Group)	Enables you to schedule a task that deploys device software to a device group. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device group for which the command is executed.
Detect Network Devices	Enables you to scan IP addresses and automatically add unknown devices to the NA database.
Detect Network Devices (Group)	Enables you to scan IP addresses and automatically add unknown device groups to the NA database.
Device Single Sign-on	Enables you o connect to device automatically via Telnet/SSH Proxy.
Discover Device Driver	Enables you to discover a device’s driver. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device for which the command is executed.
Discover Device Driver (Group)	Enables you to discover a group of devices’ driver. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device group for which the command is executed.
Drivers	Enables you to view the Drivers page. The Drivers page displays a list of the installed drivers on your system and the number of drivers currently in use.
Edit ACL	Enables you to edit ACL scripts.
Edit ACL Comments	Enables you to edit ACL comments.
Edit Config [Changed By] User	Enables you to reset the [changed by] user for a device configuration. It is recommended that this permission be set to Admin user only.
Edit Device	Enables you to change devices group membership, access device settings and other attributes. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device for which the command is executed.
Edit Device Group	Enables you to edit device groups, including adding devices to and removing devices from the device group.
Edit Inactive Device	Enables you to edit the Comments field for inactive devices.
Edit Task	Enables you to edit scheduled tasks.

Command Permission	Description
Edit User	Enables you to edit user profiles. By default, users can only edit their own user profiles.
Email Report	Enables you to schedule tasks that run various reports and send email to specified recipients.
External Authentication Setup	Enables you to setup external authentication, such as ActiveDirectory, TACACS+, SecurID, and RADIUS.
Generate Summary Reports	Enables you to schedule tasks that generate Summary reports for a single device.
Generate Summary Reports (Group)	Enables you to schedule tasks that generate Summary reports for a group of devices.
Import Devices & Passwords	Enables you to import devices and device authentication information.
List SysOIDs	Enables you to list sysOIDs of supported devices.
List View	Enables you to view the List View page. A view set of one or more partitions that separates objects in NA into specific partitions within the View.
Manage ACL	Enables you to manage device ACLs, including deleting ACLs.
Manage Command Script	Enables you to create, modify, and delete command scripts.
Manage Configuration Policy	Enables you to create, edit, and delete configuration policies.
Manage Device Password Rule	Enables you to create, edit, and delete device password rules.
Manage Diagnostic Script	Enables you to create, edit, and delete diagnostic scripts.
Manage Distributed System	Enables you to view the Distributed System pages, including the Distributed Monitor Results page, the Distributed Error List page, the Distributed Conflict List page, the List Cores page, and so on. For information on configuring a Distributed System environment, see the *NA Multimaster Distributed System on Oracle Guide*.
Manage Event Rule	Enables you to create, edit, and delete Event Notification & Response rules.
Manage Gateways	Enables you to view the Gateway List page, edit and delete Gateways, and deploy the NA Remote Agent. The NA Remote Agent includes a process that handles SNMP and coordinates with the NA Management Engine on the NA Core, a Syslog process that handles Syslog notifications from local devices, and a TFTP process that enables TFTP access to local devices.
Manage IP Address	Enables you to add, edit, and delete device IP addresses.
Manage License	Enables you to view and update NA license information.
Manage Partition	Enables you to add, edit, and delete partitions.
Manage Software Compliance	Enables you to add and/or edit software compliance information.
Manage Software Image	Enables you to add, edit, and delete software images.

Command Permission	Description
Manage Software Levels	Enables you to add and edit software compliances.
Manage System Report	Enables you to change the order of the System and User reports and delete System reports.
Manage Template	Enables you to create, edit, and delete script templates.
Manage User	Enables you to create, edit, and delete NA users.
Manage User Group	Enables you to create, edit, and delete user groups. Because user permissions are managed through this interface, this permission should be granted with care.
Manage User Role	Enables you to add, edit, and delete user roles.
Modify Device Configuration	Enables you to schedule a task that deploys an edited configuration to a device. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device for which the command is executed.
Modify SecurID	Enables you to modify SecurID token Information.
Multi-Task Project	Enables you to modify a multi-task project.
OS Analysis	Enables you to run the OS Analysis task. The OS Analysis Task page collects data about the devices, such as Information about the sysoid (unique identifier for device model), OS version, flash storage options, modules, and so on. This information is then used to make software recommendations.
Override Workflow Approvals	Enables you to run a task without going through the Workflow approval process.
Reload Device Task	Enables you to reload (reboot) a device via a reload script provided in the driver. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device for which the command is executed.
Resolve FQDNs	Enables you to schedule the Resolve FQDN task that resolves a device’s fully qualified domain name.
Resolve FQDNs (Group)	Enables you to schedule the Resolve FQDN task that resolves a device group’s fully qualified domain name.
Run Command Script	Enables you to schedule the Run Command Script task that executes a script on a specified device. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device for which the command is executed. It also requires the Script permission for the selected script.
Run Command Script (Group)	Enables you to schedule the Run Command Script task that executes a script on a specified device group. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device group for which the command is executed. It also requires the Script permission for the selected script.

Command Permission	Description
Run Diagnostic Script	Enables you to schedule the Run Diagnostic task that executes a diagnostic script on specified device. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device for which the command is executed.
Run Diagnostic Script (Group)	Enables you to schedule the Run Diagnostic task that executes a diagnostic script on specified device group. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device group for which the command is executed.
Run External Application	Enables you run a user-defined external application. This permission should be granted with care.
Run ICMP Test	Enables you to schedule the Run ICMP Test task that executes a ICMP test on a device.
Run ICMP Test (Group)	Enables you to schedule the Run ICMP Test task that executes a ICMP test on a device group.
Set Highest Priority For Tasks	Enables you to set a task’s priority to 1.
Synchronize Startup & Running	Enables you to schedule the Synchronize Startup & Running task that brings the startup & running configuration in sync for a targeted device. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission on the device for which the command is executed.
Synchronize Startup & Running (Group)	Enables you to schedule the Synchronize Startup & Running task that brings the startup & running configuration in sync for a targeted device group. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission of the device group on which the command is executed.
Take Snapshot	Enables you to schedule the Take Snapshot task that takes a device’s configuration snapshot.
Take Snapshot (Group)	Enables you to schedule the Take Snapshot task that takes a device group’s configuration snapshot.
Telnet/SSH Client	Enables you to access a device using Telnet or SSH via the NA proxy service.
Troubleshooting	Enables you to access the Troubleshooting page, send troubleshooting information via email, and change the NA server’s logging level.
Update Device Comments	Enables you to change a device’s comments.
Update Device Ticket	Enables you to configure NA to communicate with third-party ticketing systems, such as Remedy.
View ACL	Enables you to view ACL scripts.
View Command Script	Enables you to view Command scripts.
View Configuration Policy & Compliance	Enables you to view configuration policy and compliance information.

Command Permission	Description
View Configuration Policy Event	Enables you to view configuration policy event details. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission of the device for which the command is executed.
View Deployed Software	Enables you to view deployed software, as opposed to the software archive.
View Device Configuration	Enables you to view device configurations. Keep in mind that sensitive information, such as passwords and community strings, are masked.
View Device Diagnostic	Enables you to view device diagnostics.
View Device Information	Enables you to view all information related to device, except the device configuration.
View Diagnostic Script	Enables you to view diagnostic script details.
View Driver	Enables you to view driver details.
View Event Rule	Enables you to view the event rules list.
View Full Device Configuration	Enables you to view unmasked device configurations. Keep in mind this command requires both the Command permission and the corresponding Modify Device permission of the device for which the command is executed upon.
View Script & Diagnostic Result	Enables you to view the result details of a command script or diagnostic task.
View SecurID	Enables you to view SecurID token Information.
View Session	Enables you to view Telnet/SSH session command and response history.
View Software Image Archive	Enables you to view software images stored in the NA archive.
View Task	Enables you to view task details.
View Template	Enables you to view script template details.
View User Information	Enables you to view user information.
Workflow Setup	Enables you to configure Workflow approval rules.

Appendix C: Sample Scripts

This appendix contains sample scripts.

Sample PERL Script #1

This PERL script sets all FastEthernet interfaces to full duplex on Cisco 2600s and 7200s.

```
#
# Sample Script to set all FastEthernet interfaces
# to full duplex on Cisco 2600s and 7200s
#
use Socket;

$iaddr = gethostbyname("$tc_device_ip$");
$telnet_port = 23;
$sin = sockaddr_in($telnet_port, $iaddr);
socket(DEV, PF_INET, SOCK_STREAM, getprotobyname('tcp'));
connect(DEV, $sin) || die "Can't connect to $tc_device_hostname$: $!\n";

sendln("");
sendln("$tc_device_password$");
sendln("en");
sendln("$tc_device_enable_password$");
sendln("conf t");

for $name (split(" ","$tc_device_port_name_list$")) {
  if ($name =~ /FastEthernet/)
      sendln("interface $name");
      sendln("duplex full");
      sendln("exit");
   }
}
sendln("exit");
sendln("exit");
sendln("");
close(DEV);
exit;
```

(continued on next page)

```
sub sendln {
  my ($line) = @_;
  $line .= "\n";
  syswrite(DEV,$line,length($line));
  while (<DEV>) {
   print;
  die "Failed to execute command\n"
    if (/\% (Unknown|Unrecognized|Invalid|.*uthorization failed)/);
  last if (/name:/ ||
         /word:/ ||
         />/ ||
         /\#/);
  }
}
```

Sample PERL Script #2

This PERL script sets all interfaces to no IP-directed broadcast.

```
#
# Sample Script to set all interfaces
# to no ip directed broadcast
#
use Socket;

$iaddr = gethostbyname("$tc_device_ip$");
$telnet_port = 23;
$sin = sockaddr_in($telnet_port, $iaddr);
socket(DEV, PF_INET, SOCK_STREAM, getprotobyname('tcp'));
connect(DEV, $sin) || die "Can't connect to $tc_device_hostname$: $!\n";

sendln("");
sendln("$tc_device_password$");
sendln("en");
sendln("$tc_device_enable_password$");
sendln("conf t");

for $name (split(" ","$tc_device_port_name_list$")) {
   sendln("interface $name");
   sendln("no ip directed-broadcast");
   sendln("exit");
}
sendln("exit");
sendln("exit");
sendln("");
close(DEV);
exit;

sub sendln {
  my ($line) = @_;
  $line .= "\n";
  syswrite(DEV,$line,length($line));
  while (<DEV>) {
    print;
    die "Failed to execute command\n"
      if (/\% (Unknown|Unrecognized|Invalid|.*uthorization failed)/);
    last if (/name:/ ||
           /word:/ ||
          />/ ||
         /\#/);
```

Sample Expect Script

This Expect script modifies the banner to contain a given string only if the banner does not already contain the string.

```
#
# Sample Script to set the banner only if
# it is not already set correctly
#
spawn telnet $tc_device_ip$
set banner "****Unauthorized Access Prohibited****"
expect {
   $banner {
      puts "\nBanner is already set correctly\n"
      exit 0
   } "word:"
}
send "$tc_device_password$\r"
expect ">"
send "en\r"
expect "word:"
send "$tc_device_enable_password$\r"
expect "\#"
send "config t\r"
expect "\#"
send "banner motd /$banner/\r"
expect "\#"
send "exit"
```

Glossary

This Glossary includes definitions of HP Network Automation (NA) terminology. The terms are listed in alphabetical order.

Term	Definition
Core	A single NA Management Engine, associated services (Syslog and TFTP), and a single database. A Core can manage multiple Sites (set of devices).
Device Password Rule	Enables you to apply the same username, password, and SNMP community strings to groups of devices, IP address ranges, or host names.
Default Site Partition	The default Partition is named Default Site). If you are new to NA, the default Partition is the only Partition available. It includes all of the devices currently managed by NA.
Device View	A View that applies to devices and device groups.
Diagnostic	A command that is run on a device to collect information about the device that is not captured in its configuration file. For example, on a Cisco router, a Diagnostic would be the output of the command Show NTP Status.
Distributed System	A system with more than one Core, with each Core running on a separate server.
Gateway	An application that routes IP traffic to other Gateways. The Gateway software enables you to manage servers behind NATed devices and firewalls. In addition, the Gateway supports bandwidth throttling on tunnels between Realms and can be used anywhere SSL proxying or TCP port forwarding is used. Tunnels can be authenticated and optionally encrypted using SSL.
Multimaster	A system with more than one database, where each database contains a complete set of all data.
Multi-Task Project	A multi-task project can run several different tasks sequentially joined together under a single project. Each task included in the multi-task project is run in the order you specify.
Parent Group	A device group hierarchy in NA is made up of parent groups and Leaf groups. A parent group can only have one parent. A parent group can contain only device groups, not devices.

Term	**Definition**
Partition	Partition are a set of NA objects. NA objects can include devices, users, command scripts, device password rules, policies, software images, and so on. Partitions can also be used in conjunction with a permissions model, group hierarchy, distribution of devices across NA Cores, and network diagramming.
Policy	A collection of rules that test the configuration and run-time state of your devices.
Realm	A network segment. In general, a Realm is identified by a set of unique IP addresses. For example, a Realm cannot contain two devices numbered as 10.255.111.128. Instead, the devices must be broken out into separate Realms. A Site is not required to be in the same Realm as its managing NA Core.
Role	Roles are used to partition users into groups that share the same security privileges. A user assigned to a role is granted permissions defined by the role. For example, if a user is authorized to perform certain operations, such as adding devices, managing configuration policies, or deploying software, NA uses fixed role identities with which to access resources.
Rule	An automated test that validates at least one of the following: • Specific configuration settings • Specific data model element • The run-time state of a device (also known as a Diagnostic) • The software version running on a device
Rule Exception	A rule exception is part of a rule. However, its purpose is to exclude text it matches in the device configuration from consideration by the rule it is part of.
SingleSearch	The SingleSearch option enables you to search all events containing the specified search criteria you specify on the SingleSearch Results page.
SingleView	SingleView enables you to track events that indicate changes to either a single device or all of your devices on one page.
Tasks	The primary mechanism by which NA interacts with your network. Tasks are specific actions you can either schedule or run immediately, for example Deploy Passwords, Reload Device, and Task Snapshot.

Term	Definition
Task Pool Initialization	When the NA management engine starts, it queries the database to construct the Task Pool. When a task is created, updated, or deleted, NA only updates the database which is attached to the local NA Core. The database replication mechanism handles the necessary changes in the databases attached to remote NA Cores. However, it is the application's responsibility to call remote NA Cores to update their the Task Pool in memory.
User Group	A logical container for the purpose of user management. The System Administrator can assign users to user groups, which in turn map to specific roles.
User View	View that applies to users and user groups
Workflow	The NA Workflow Integration & Routing Engine (WIRE) manages the process of network configuration, ensuring that network changes are made according to predefined policies, completed in the correct sequence, and approved by the appropriate people.

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click *here*.

If no email client is available, copy the information below to a new message in a web mail client, and then send this message to **ovdoc-nsm@hp.com**.

Product name and version: NA 9.21

Document title: *NA User Guide, December 2012*

Feedback: