Device Driver Reference for Network Compliance Manager 1.x

CiscoWorks

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-10252-13

Device Driver Reference for Network Compliance Manager

Table of Contents

Getting Started

The *Device Driver Reference for Network Compliance Manager (NCM) 1.x* contains the list of supported devices and device details supported by NCM.

Supported Devices

NCM supports the following devices. The list is in alphabetical order.

Vendor	Model	OS Version
3Com	SuperStack II Switch 3300	2.x
3Com	SuperStack III Switch 4400	3.x
3Com	Switch 5500	3.2
Adtran	NetVanta 3000 Series Router	07.x, 14.4
Adtran	Atlas routers 550 and 890	C.08x
Alcatel	OmniSwitch 6000 Series	5.3.x.x.x
APC	MasterSwitch 7900 Series	2.2.x, 2.6.x
Arris	Cadant C4 CMTS	04.02
Aruba	Mobility Controller 5000 Series	2.x
Audiocodes	Mediant 2000	5.00A.024
Avaya	Switch P330	4.5x
BelAir	Access point 100 Series	6.x
BelAir	Access Point 200 Series	2.0
Blue Coat	ProxySG 600 Appliance	3.x
Cabletron	SmartSwitch 6C105, 6E132-25, 6E132-25-A621, 6H202-24, 6H252-17	5.0.8.04
Cabletron	SmartSwitch 2E48-27R	4.11.26
Check Point	FireWall-1, Nokia	NG Feature Pack 3
Check Point	Provider-1 CMA, Linux	NGX R61

Vendor	Model	OS Version
Check Point	FireWall-1, Solaris	NG Feature Pack 3
Check Point	SecurePlatform, Linux	NG Feature Pack 3
Ciena	CN 2000 Storage Extension Platform	4.x
Cisco	ACE Application Control Engine Module	3.0
Cisco	Access Server AS2511	12.3
Cisco	Access Server AS5400 Series Universal Gateway	12.x
Cisco	ADSL Router 800	12.x
Cisco	Aironet 340	11.23T & 12.01T1
Cisco	Aironet 350	11.23T, 12.01T1 & 12.2
Cisco	Aironet 1100, 1200	12.2
Cisco	Aironet 1240AG, 1300	12.3
Cisco	Content Engine 500 Series (ACNS)	5.1.15, 5.3.3, 5.5.5
Cisco	ASA 5500 Series Adaptive Security Appliance	7.0, 7.1
Cisco	BPX Switch 8600 Series	9.4.10
Cisco	Catalyst Router Module MSFC, Module RSM	11.x, 12.x
Cisco	Catalyst Blade Switch (CBS)	12.x
Cisco	Catalyst Switch 1900	9.x Standard Edition
Cisco	Catalyst Switch 2820, 2900	5.x, 6.x & 7.x
Cisco	Catalyst Switch 2900XL	11.x, 12.x
Cisco	Catalyst Switch 2900XL, 3500XL, 4908G-L3/GESM	12.x
Cisco	Catalyst Switch 2940	12.x
Cisco	Catalyst Switch 2948	11.x, 12.x
Cisco	Catalyst Switch 2948G-GE-TX	5.x, 6.x & 7.x
Cisco	Catalyst Switch 2950, 2950-24, 2950-24C/G	12.x
Cisco	Catalyst Switch 2950-48T and 2950T-24	12.x
Cisco	Catalyst Switch 2960 and 2970	12.x
Cisco	Catalyst Switch 3500XL, 3548XL	11.x, 12.x
Cisco	Catalyst Switch 3550, 3560, 3750	12.x
Cisco	Catalyst Switch 4000, 4500	5.x, 6.x & 7.x

Vendor	Model	OS Version
Cisco	Catalyst Switch 4000, 4500, 6000 (Native Mode)	11.x, 12.x
Cisco	Catalyst Switch 4908G-L3	11.x, 12.x
Cisco	Catalyst Switch 4948	12.x
Cisco	Catalyst Switch 5000, 5500	5.x & 6.x
Cisco	Catalyst Switch 6000	5.x, 6.x. 7.x & 8.x
Cisco	Catalyst Switch 6500	5.x, 6.x & 7.x
Cisco	Catalyst Switch 6000, 6500 (Native Mode)	11.x, 12.x
Cisco	Catalyst Switch 6500 Services Module (FWSW)	3.1(1)
Cisco	Catalyst Switch 6500 Wirless Services (WiSM)	4.0.x, 4.1.x
Cisco	Catalyst Switch 8500	12.x
Cisco	CMTS uBR7200 Series, uBR10000 Series	12.x
Cisco	Content Services Switch CSS 11000	4.x, 5.x & 6.x
Cisco	Content Services Switch CSS 11500	7.x
Cisco	Content Switch Local Director 400 Series	12.x
Cisco	FastHub 400 series	1.0
Cisco	Global Site Selector (GSS)	1.2, 1.3
Cisco	Intelligent Gigabit Ethernet Switch Module (IGESM) for the IBM BladeCenter	12.x
Cisco	LightStream 1010, 1015	12.x
Cisco	Load Balancers, LD Series	
Cisco	ONS 15454	5.4, 6.02.02
Cisco	MC3810 Multiservice Concentrator	12.x
Cisco	MDS Multilayer Switch 9000 Series	2.0, 2.1, 3.1
Cisco	Modular Access Platform 3662	12.x
Cisco	ONS 15530, 15540	12.x
Cisco	ASA 5500 series Adaptive Security Appliance	7.0
Cisco	PIX Firewall 500 Series	5.x, 6.x & 7.x
Cisco	Riverhead Guard Firewall	3.x
Cisco	Router 800 and 1000	11.x, 12.x
Cisco	Router 7140-2AT3	11.x, 12.x

Vendor	Model	OS Version
Cisco	Router 1600, 1700, 1800, 2500, 2600, 2800	11.x, 12.x
Cisco	Router 3600 3700, 3725, 3800	11.x, 12.x
Cisco	Router 4000, 4500	11.x, 12.x
Cisco	Router 4700	11.x, 12.x
Cisco	Router 7000, 7100, 7200, 7300, 7500, 7606	11.x, 12.x
Cisco	Router 7604	11.x, 12.x
Cisco	Router 7606 (CatOS)	5.x, 6.x & 7.x
Cisco	Router 7606 (IOS)	11.x, 12.x
Cisco	Router 7609	12.x
Cisco	Router 7613/Router 12000 GSR	11.x, 12.x
Cisco	Router 12000 XR (IOS XR)	3.2.1
Cisco	Router AS 5200, 5300	12.x
Cisco	Router CRS-1 (IOS XR)	3.4, 3.5
Cisco	SOHO 9x Series Router	12.x
Cisco	Switch 1548 series	12.x
Cisco	Switch ME2400, ME3400	12.x
Cisco	Voice Gateway VG248	1.3
Cisco	VoIP Gateway VG200 Series	12.x
Cisco	VPN Concentrator 3000	3.x, 4.7.x
Cisco	Wide Area Application Engine (WAE)-611, 612	4.x
Cisco	Wide Area Application Engine (WAE) 7300	5.3.3
Cisco	2000, 4100, 4400 Series Wireless LAN Controller	2.2.x, 3.2.x, 4.0.x, 4.1.x
Citrix	NetScaler 9000 Series Switch	6.x
Colubris	MAP-320/330	5.1.3
Comtech	Satellite Modem SLM-5650	1.04.02
Crossbeam	C-Series Security Services Switch	3.0.1-15
Cyberguard	Firewall FS 300/600, KS 1000/1500	5.2
Cyclades	Terminal Server TS400, TS1000	1.3.x, 1.4.x
Cyclades	Terminal Servers, Device Series	2.6.x, 3.0

Vendor	Model	OS Version
Cyclades	Terminal Server TS Series	1.4.x
Dell	PowerConnect Switch 3448P	1.0.1.13, 2.1.0.0
Dell	PowerConnect Switch 3248, 6248	1.x, 2.x
Digi	PortServer TS 8/16 MEI, TS 16 Rack	82000684_T/T1
Edgewater Edgemarc	Device Series 4200, 4300, 4500, 5300	6.x
Enterasys	Matrix E-Series	2.2
Enterasys	Matrix SecureStack	4.0.x, 5.0.x
Enterasys	SSR-2000 SmartSwitch Router	3.0.x
Enterasys	Matrix Switch SecureStack C2 Series	4.0.x, 5.0.x
Enterasys	X-Pedition 8000 SmartSwitch Router	9.x
Expand	Accelerator 4000 Series	4.5
Extreme	Alpine 3804	6.2.x, 7.x
Extreme	Alpine 3808	6.2.x, 7.x
Extreme	Alpine Series	7.x
Extreme	Black Diamond Series	6.x, 7.x
Extreme	Black Diamond Series 8800, 10808, 12804R, 12804C Series (ExtremeXOS)	11.3.x, 11.4.x, 11.5.x, 11.6.x
Extreme	Summit X450, X450a Series (ExtremeXOS)	11.3.x, 11.4.x, 11.5.x, 11.6.x
Extreme	Summit 24/48	4.1
Extreme	Summit Series	6.x, 7.x
F5	3-DNS Traffic Management Controller	4.x
F5	BIG-IP Load Balancer	4.x, 9.x
Fore Systems	Switch ASX1000	5.3.1
Foundry	FastIron Edge Switch	3.x
Foundry	FastIron Workgroup Switch, NetIron Switch	7.x
Foundry	ServerIron Switch	7.x, 8.x
Force10	Router E-Series	5.x
Funkwerk	Artem W3000 Series Access Point	6.05
HP	ProCurve 2500	F.05.x

Vendor	Model	OS Version
HP	ProCurve 2600	F.07.x, H.08.106, H.10.35, H.10.36
HP	ProCurve 3500, 5406, 5412	11.x, 12.x
HP	ProCurve 5308x1	E.08.x
HP	ProCurve M-Series	08.x, 09.x
HP	ProLiant Switch Series	2.0
Intel	Sarvega Guardian Gateway	5.1.x
Huawei	Quidway AR 28-31 Router	3.4
Huawei	Quidway NetEngine routers/switches	3.x, 5.x
Juniper	Juniper CTP 2008/2056 Series	4.1R11
Juniper	DX Series Application Accelerator	5.0.x
Juniper	Routers	5.5, 6.x, 7.x, 8.0.x, 8.1.x
Juniper	NetScreen-5GT Firewall/VPN, ADSL Firewall/VPN	5.x
Juniper	NetScreen-5GT Wireless Firewall/VPN	5.x
Juniper	NetScreen-5XP Firewall/VPN	2.6.1, 5.x
Juniper	NetScreen-5XT Firewall/VPN	5.x
Juniper	NetScreen-25, 50, 204 Firewall/VPN	5.x
Juniper	NetScreen-208 Firewall/VPN	2.6.1, 5.x
Juniper	NetScreen-500, 5200/5400 Firewall/VPN	5.x
Juniper	NetScreen-500 GPRS Firewall/VPN	5.x
Juniper	NetScreen-HSC Firewall/VPN	5.x
Juniper	J-Series J6300	8.x
Juniper	NetScreen-ISG 1000, 2000 Firewall/VPN	5.x, 5.4.12
Juniper	Secure Services Gateway SSG 5, 20, 520, 520M, 550, 550M	5.4.12
Juniper	Session Border Controller VoiceFlow 3000	5.3.x 6.0.x
Juniper	T-Series T640	5.5, 6.x, 7.x, 8.x
Juniper	WX/WXC Application Accelerator	5.x
Lantronix	Ethernet Terminal Servers ETS8P/ETS16P	V3.6/4
Lucent	Router MAX 6000	7.4.x

Vendor	Model	OS Version
Maipu	1762, 2700, 3000 series routers	3.x, 5.x
Marconi	ATM Switch ASX-1000, ASX-1200, ASX-4000	6.2 & 8.0
Marconi	ATM Switch ASX-200BX, ASX-200BXE	6.2 & 8.0
Motorola	PathBuilder 2500, 4000, 6000	11.x, 14.x, 15.0
NEC	IX5000 Series Switch	7.x and higher
NEC	Univerge 2000 Series Routers	5.x, 7.x
NET	NETScream 50/100	X
Netopia	3300 Series Router	4.8.x, 8.x
Network Appliance	Proxy NetCache Series	7.x
Network Appliance	Proxy NetCache C720, C720S, C1100, C1105, C3100	5.5x
Nortel	Alteon 180 and Alteon ACEdirector (AD) Series	WebOS 10.0
Nortel	Alteon Application Switch (AAS) 3408	22.0.x, 234.0.3
Nortel	Alteon ASF	3.5
Nortel	Alteon SSL-VPN	4.2.1, 5.0
Nortel	Alteon SSL Accelerator/VPN Gateway 3050 and 3070	4.2.1, 6.x, 6.05
Nortel	BayStack 325	3.0, 3.5
Nortel	BayStack 380	3.0
Nortel	BayStack 350T, 450T	4.x
Nortel	BayStack 420	3.0, 3.1.1.01
Nortel	BayStack 425	3.0, 3.1, 3.6
Nortel	BayStack 460	2.2, 3.0
Nortel	BayStack 470	2.2, 3.0, 3.1, 3.5, 3.6
Nortel	BayStack 5500 Series	2.2, 3.0, 3.1, 4.0, 4.1, 4.2, 4.3, 5.0
Nortel	BayStack BPS2000	1.1.3.x, 3.0, 3.1
Nortel	Contivity 100, 400	7.20
Nortel	Contivity 600, 1000 series	4.x, 5.x, 6x
Nortel	Contivity 1700 Series	4.x, 5.x

Vendor	Model	OS Version
Nortel	Contivity 2000, 4000 and 5000 Series	4.x
Nortel	Centillion ATM Switch, 50/100 Series	3.x
Nortel	Ethernet Routing Switch 2500 Series	4.0
Nortel	Ethernet Routing Switch 4500 Series	5.0
Nortel	GbE Switch Module for IBM BladeCenter	1.0.x, 1.2.x
Nortel	OPTera Metro Ethernet Service Modules	1.2, 1.3.5
Nortel	Passport 1200	2.1.6.1
Nortel	Passport 1600	1.1, 1.2.4, 2.1
Nortel	Passport 6400	CB02S1B
Nortel	Passport 8000, and ERS routers, 1600/8000	3.2, 3.3, 3.4, 3.5, 3.7, 4.1
Nortel	Passport 8300	3.0
Nortel	Passport 8600	3.2, 3.3, 3.4, 3.5, 3.7, 4.1
Nortel	Router AN, ARN, ASN, BCN, BLN, BN	14.03, 14.20, 15.4 & 15.5, 15.6, 15.7, 15.6.3.2
Nortel	Router Passport 2430, 5430	14.03, 14.20, 15.4 & 15.5
Nortel	Secure Router (Tasman) 1001	8.1, 8.2, 8.2.1
Nortel	Secure Router (Tasman) 1002, 1004	7.0.5, 7.11, 7.2, 7.2b, 7.3, 8.0, 8.0.1, 8.2, 8.2.1, 8.4
Nortel	Secure Router (Tasman) 1400	8.0, 8.0.1
Nortel	Secure Router (Tasman) 3120	9.0
Nortel	Secure Router (Tasman) 4100	7.2b, 8.2.1
Nortel	Secure Router (Tasman) 6302	8.2.1
Nortel	VPN Router 1700/1740/2700/5000 series	07.00.062
Nortel	WLAN Access Point 2220	1.2
Nortel	WLAN Security Switch 2250	1.0
Nortel	WLAN Switch 2270 Series	2.0
Nortel	WLAN WWS Switch 2330, 2350, 2360, 2361 series	5.0, 5.0.11.4
Packeteer	PacketShaper	6.x, 7.x, 8.x
Paradyne	IP DSLAM 4229 Series	2.x
Powerware	ConnectUPS Web/SNMP Card	V4.18, V1.37

Vendor	Model	OS Version
Procket	Pro/8000 Series	2.x
Qualcomm	Flarion RadioRouter RR2045	2.11.x and higher
Radware	LinkProof	4.35.06, 4.35.07
Radware	Load Balancer AppDirector	1.03.04
Riverbed	Steelhead 520, x010 series	3.x
Riverstone	RS2000, Cabletron OEM SSR2000 Switch Router	E9.0.7.7
Secure Computing	Sidewinder G2	6.x
Sonus	Sonus GSX	06.03.02 R004
Symbol	ES3000 switch	v1.0.0.0-915R, 1.0.2
Symbol	Spectrum Access Point, AP-302x	04.02
Symbol	Spectrum24 Access Point, AP-4100	02.x, 03.x
Symbol	WS2000 Wireless Switch	1.5.x, 2.2.x
Terayon	CMTS Gateway and CMTS TL1000	1.39
Transition	CPSMM100-120	060117PQ
TrippLite	PowerAlert	12.04.0019
Various	UNIX Servers	Linux, FreeBSD, SunOS
Yamaha	RTX1100 Router	8.03.46
ZyXEL	ZyWALL 2X Firewall/VPN Router	3.62
ZyXEL	ZyAIR G-2000 Plus Wireless Router	3.62

AAA Configuration

To implement AAA change detection, NCM installs an agent on your AAA server. The agent parses the logs of the AAA application and forwards appropriate logs to NCM over port 1099. From the AAA logs, NCM can detect when a user logs in and out of devices, enabling NCM to report who made a change and when.

The agent causes minimal load on your AAA server. The agent makes only outbound connections. It does not accept incoming connections and does not open any security holes on the server.

NCM supports CiscoSecure ACS directly. For help configuring AAA, or if you use another AAA server, contact Customer Support.

Note: *If your network already uses Radius or TACACS+, you should create a separate user name and password for NCM. If you do this, put the Radius or TACACS+ user name in the AAA User Name field on the Edit User page.*

Protocols and Ports

NCM communicates with network devices using a combination of the protocols listed in the table below. If a firewall is present between the NCM server and the network devices, you must provide NCM access to the devices by opening the ports used by those protocols.

	Port		
Protocol	**Windows**	**Solaris**	**Use**
SSH (TCP)	22	8022	NCM server to network devices
telnet (TCP)	23	8023	NCM Server to network devices
TFTP (UDP)	69	69	Network devices to TC Server
SNMP (UDP)	161	161	NCM Server to Network devices
SNMP trap (UPD)	162	162	NCM Server to NMS
syslog (UDP)	514	514	Network devices to TC Server
JNDI	1099	1099	AAA Server to TC Server
RMI	4444	4444	AAA Server to TC Server

Inline Comment Characters

If you use the NCM user interface, NCM displays the inline comment characters at the top of the Edit Configuration page. If you use the CLI or write scripts, use the following table as a reference.

Note: *If the you do not use a double comment character when commenting the configuration in NCM, either the device or NCM could overwrite the user's comments.*

Platform	Characters	Description
3COM	NA	SuperStack II
Check Point	##	All deployable configurations
Cisco Aironet	##	340 and 350 series
Cisco Aironet	!!	1100 and 1200 series
Cisco CatOS	##	2948G, 2980, 4000, 5000, and 6000 series (hybrid mode)
Cisco IOS	!!	All deployable configurations
Cisco VPN	##	VPN Concentrator 3000 series
Extreme Summit	##	24 and 48
F5 Networks	##	BIG-IP and 3DNS
Foundry	!!	NetIron series
Marconi	##	Devices running ForeOS
NetScreen	##	5XP
Nortel Routers	##	BayRS series
Nortel Switches	##	BayStack 350, 410, 420, 425, 450, and 470; Passport 8000 series
Nortel VPN	!!	Contivity 100, 2600, 4500, 4600

See “Device Details” for which comment characters are used.

Using Documentation Resources

NCM comes with ample documentation. To open any of the available PDF documents, when logged-in, on the menu bar click Docs. The CiscoWorks Network Compliance Manager Documentation page opens. NCM also has online Help that you can access via the Help link at the top of each page.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Viewing the Software Version

The About CiscoWorks Network Compliance Manager page provides information about this software version. The page also includes links to other important pages, such as License Information, Feedback, and Customer Support. In addition, you can see the list of device drivers installed on your system.

On the menu bar under Admin, click About CiscoWorks Network Compliance Manager. The available links from the About CiscoWorks Network Compliance Manager page include:

- Download Driver Update Packages
- View Latest Release Notes
- View License Information
- Create Technical Support Ticket
- Email Customer Support
- Request New Driver Support

Sending Feedback

Cisco values your feedback on our product. On the About Network Compliance Manager page, you can click the Email Customer Support or the Create Technical Support Ticket links. If you are submitting a technical issue, be sure to include the following information and click Submit or Reset when done.

- Reply-to Email Address: The email address you want us to reply to.
- Subject, Reference: The subject of your feedback.
- Subject, Other: If the reference list does not include the subject you want, type your own subject here.
- Message: Enter your comments here. Include as much context as possible so we can respond quickly and appropriately to your feedback.
- Operating System: Choose the operating system on the computer on which the NCM Management server runs.
- CPU: Choose the CPU type of the computer on which the NCM Management server runs.
- CPU Frequency: Choose the CPU speed of the computer on which the NCM Management server runs.
- Number of CPUs: Choose the number of CPUs of the computer on which the NCM Management server runs
- System Memory: Choose the total RAM on the computer on which the NCM Management server runs.
- Free Memory: Choose the RAM available on the computer on which the NCM Management server runs.
- Free Disk Space: The disk space available on the computer on which the NCM Management server runs.
- Display Resolution: Choose the screen resolution used on the NCM client computer. NCM looks best using 1024x768 or higher.
- Database: Choose the database you are using with NCM.
- Send a CLI Log?: Select this box to send a CLI log as an attachment to your feedback email message.

Driver Details

CiscoWorks Network Compliance Manager (NCM) detects device changes using Syslog notifications, among other methods. For NCM to detect device changes, you must either enable NCM to configure Syslog automatically (the default) or enable logging on each device using the device settings detailed in the following sections. All standard features and protocols work as expected in NCM unless otherwise noted.

3COM SuperStack II switches, OS version 2.x

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment	X	
Diagnostics		
Routing Table		
OSPF Neighbors		
Interfaces	X	
Modules and Inventory	X	
Flash Storage Space		
File System		
Uptime		X
ICMP Test	X	
Topology Parsing	X	
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management (can modify full username and full password)	X	
Syslog Configuration and Change Detection		

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Known Issues

Device configuration consists of diagnostic results and cannot be deployed

The device does not have any canonical configuration file or output. Consequently, NCM captures the output of a number of device diagnostics that provide information about the device's current configuration. This collected information is not in a format that can be restored to the device directly. Therefore, configuration deployment is not supported.

Change password task may fail, but appear to succeed

To change the password for a user, the user must exist in NCM. NCM will not create a new user account and create a password. However, NCM can report a successful password change because the device does not report a problem with NCM’s attempt to change the password.

User's password and SNMP community string cannot be changed simultaneously

The operating system on the device associates users with levels (such as manager, monitor, and security), and associates an SNMP community string with a user account. An SNMP community string cannot exist without an associated user account. When changing passwords, the operating system offers to change the SNMP community string at the same time. NCM does not modify the SNMP community string for a user whose password was just changed.

Real-time change detection available only through Telnet/SSH proxy

The device does not support Syslog or AAA and therefore cannot provide any real-time change detection through those means. The Telnet/SSH proxy is the only mechanism in NCM that will result in automatic detection of changes to the device configuration.

Multi-line commands are ignored by the device

The device ignores multi-line commands (commands that require multiple lines of input before returning to the device prompt). Issuing a command such as "snmp comm\r\nc1\r\n" results in the execution of the "snmp comm" command. Everything else in the command line is ignored.

Workaround:

The device automatically fills any subsequent prompting of a command with the next item on the original command line. Consequently, the command "snmp comm c1" automatically answers the first prompt from the "snmp comm" command with "c1".

To get the device to properly return to a device prompt (and thereby not result in a failed script), an answer to every prompt the command might issue must be provided on the original command line.

3COM SuperStack 3 switches, OS version 3.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X		X
Configuration			
Configuration Snapshot (Startup configuration captured: no)			X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running)	X		
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System			
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center	X		
Password Management (can modify full username and full password)	X		

FEATURE	CLI	SNMP	TFTP/CLI
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Known Issues

Configuration Deployment may cause duplicate configuration options

Deploying certain configuration commands may cause the device to produce multiple duplicate configuration lines. For example, the “system management snmp trap create” command has been seen to generate multiple configuration statements.

Workaround:

Unless you are creating a new configuration using a similar command, remove commands such as the “system management snmp trap create” command from the configuration before deploying the configuration to the device.

Real-time change detection available only through Telnet/SSH proxy

The device does not support Syslog or AAA, and therefore cannot provide any real-time change detection through those means. The Telnet/SSH proxy is the only mechanism in NCM that will result in automatic detection of changes to the device configuration.

3Com 5500EI 24 port switch, OS Version 3.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to startup with reboot)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime			
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify full username, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Known Issues

Strict password controls require synchronization of passwords

The 3Com 5500EI 24 port switch implements strict password controls that limit NCM to a single Administrative user. This username is mutable, however its password is automatically synchronized with the super or enable password. Additionally, user passwords are maintained in a history file and therefore must remain unique upon subsequent deployments.

Adtran Atlas routers, Models 550 and 890, OS version C.08.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)			X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment			X
Diagnostics			
Routing Table			
OSPF Neighbors			
Interfaces			
Modules and Inventory			
Flash Storage Space			
File System			
Uptime		X	
ICMP Test			
Topology Parsing			
Duplex Mismatch Parsing			
Other			
Software Center			

FEATURE	CLI	SNMP	TFTP/CLI
Password Management			
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics			
ACL Management			
Configlet Parsing			

Adtran NetVanta routers, OS version 07.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X		X	
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destinations: to running, to startup with reboot)			X	
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory				
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing				
Other				
Software Center	X			

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Alcatel OmniSwitch Switch, 6000 Series, OS version 5.3.x.x.x

FEATURE	CLI	SNMP	FTP	FTP/CLI
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X		X
Configuration				
Configuration Snapshot (Startup configuration captured: no)	X			
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destination: to startup with reboot))			X	
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory				
Flash Storage Space				
File System	X			
Uptime				
ICMP Test	X			
Topology Parsing				
Duplex Mismatch Parsing				
Other				

FEATURE	CLI	SNMP	FTP	FTP/CLI
Software Center	X			X
Password Management (limited password)	X			
Syslog Configuration and Change Detection				
Custom Scripts and Diagnostics	X			
ACL Management				
Configlet Parsing				

Known Issues

Changing the login password using SSH

When attempting to change the login password using SSH as the access protocol on the Alcatel OmniSwitch 6000 series, you could encounter an internal error. Note that this issue has not been observed when using Telnet as the access protocol.

Deploying Configurations

If you edit one command of a stored configuration on an Alcatel device and then deploy just that configuration command change without deploying the entire configuration, the one command change replaces the entire configuration.

APC Master Switch, 7900 Series, OS version 2.2x

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table	X	
OSPF Neighbors		
Interfaces		
Modules and Inventory	X	
Flash Storage Space		
File System		
Uptime		X
ICMP Test	X	
Topology Parsing		
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management (can modify: full username, full password)	X	

FEATURE	CLI	SNMP
Syslog Configuration and Change Detection	X	
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Arris Cadant CMTS, C4, CMTS_V04.02dtran NetVanta

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: yes)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to running, to startup with reboot)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Aruba Mobility Controller, 800 & 5000 Series, OS version 2.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X		X	
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destinations: to startup with reboot)			X	
Diagnostics				
Routing Table	X			
OSPF Neighbors				
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing				
Other				

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Software Center	X			
Password Management (can modify: limited password, full password, read-only community strings, read-only community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Audiocodes Mediant 2000, v. 5.00A.024

FEATURE	CLI	SNMP	Other
Driver Discovery		X	
General Access (CLI protocols: Telnet, SSH2, Console)	X	X	HTTP
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running)			HTTP
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces			
Modules and Inventory			
Flash Storage Space			
File System			
Uptime		X	
ICMP Test	X		
Topology Parsing			
Duplex Mismatch Parsing			
Other			
Software Center			HTTP
Password Management (can modify: full username/ password, read/write community strings)	X		HTTP

FEATURE	CLI	SNMP	Other
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Known Issues

Updating SNMP Community Strings

You must reboot the Audiocodes Mediant 2000 for SNMP community strings changes to take effect.

Using HTTPS

Using HTTPS for a secure HTTP connection on the Audiocodes Mediant 2000 is unreliable and could cause improper functionality. For example, the Edit/ Delete ACLs task only works with HTTP.

Avaya P330 Switch, OS version 4.5.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery			
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)			X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment			
Diagnostics			
Routing Table			
OSPF Neighbors			
Interfaces			
Modules and Inventory			
Flash Storage Space			
File System			
Uptime			
ICMP Test			
Topology Parsing			
Duplex Mismatch Parsing			
Other			
Software Center			
Password Management			

FEATURE	CLI	SNMP	TFTP/CLI
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

BelAir access points, 50 and 100 series, OS version 6.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X		X
Configuration			
Configuration Snapshot (Startup configuration captured: no)			X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to startup with reboot)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System	X		
Uptime			
ICMP Test	X		
Topology Parsing			
Duplex Mismatch Parsing			
Other			
Software Center			

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: full username, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

BlueCoat ProxySG, OS version 3.x

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment (destination: to running)	X	
Diagnostics		
Routing Table	X	
OSPF Neighbors		
Interfaces	X	
Modules and Inventory	X	
Flash Storage Space		
File System		
Uptime		X
ICMP Test	X	
Topology Parsing		
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management (can modify: limited username, limited password, full password, read-only community strings, read/write community strings)	X	

FEATURE	CLI	SNMP
Syslog Configuration and Change Detection	X	
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Known Issues

Unable to discover driver via Telnet

The BlueCoat ProxySG has a default banner for Telnet logins that causes driver discovery to fail to recognize the device. As a result, discovery via Telnet will always fail on the BlueCoat ProxySG. Discovery via SNMP or SSH will work correctly.

Changes in community strings not detected

The BlueCoat ProxySG encrypts community strings in its configuration. This encryption scheme results in a changed encrypted community string with every snapshot. These changes are masked out to prevent every snapshot from indicating a change, but actual changes to SNMP community strings will therefore not be detected.

Cabletron SmartSwitch 6C105

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, Console)	X	
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table		
OSPF Neighbors		
Interfaces		
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		
ICMP Test		
Topology Parsing		
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management (can modify: full password, read-only community strings, read/write community strings)	X	
Syslog Configuration and Change Detection		

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics		
ACL Management		
Configlet Parsing		

Cabletron SmartSwitch 6H252-17

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, Console)	X	
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table		
OSPF Neighbors		
Interfaces		
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		
ICMP Test		
Topology Parsing		
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management (can modify: full password, read-only community strings, read/write community strings)	X	
Syslog Configuration and Change Detection		

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics		
ACL Management		
Configlet Parsing		

Cabletron SmartSwitch 6H202-24

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, Console)	X	
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table		
OSPF Neighbors		
Interfaces		
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		
ICMP Test	X	
Topology Parsing		
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management (can modify: full password, read-only community strings, read/write community strings)	X	
Syslog Configuration and Change Detection		

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics		
ACL Management		
Configlet Parsing		

Cabletron SmartSwitch 6H122-08

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, Console)	X	
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table		
OSPF Neighbors		
Interfaces		
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		
ICMP Test	X	
Topology Parsing		
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management (can modify: full password, read-only community strings, read/write community strings)	X	
Syslog Configuration and Change Detection		

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics		
ACL Management		
Configlet Parsing		

Cabletron SmartSwitch 2E48-27R

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, Console)	X	
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table		
OSPF Neighbors		
Interfaces		
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		
ICMP Test	X	
Topology Parsing		
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management (can modify: full password, read-only community strings, read/write community strings)	X	
Syslog Configuration and Change Detection		

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics		
ACL Management		
Configlet Parsing		

Cabletron SmartSwitch 6E132-25-A621, 6E132-25

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, Console)	X	
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table		
OSPF Neighbors		
Interfaces		
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		
ICMP Test	X	
Topology Parsing		
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management (can modify: full password, read-only community strings, read/write community strings)	X	
Syslog Configuration and Change Detection		

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics		
ACL Management		
Configlet Parsing		

Carrier Access Corporation (CAC) Adit, 600, OS version 9.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to running)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces			
Modules and Inventory	X		
Flash Storage Space			
File System			
Uptime			
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center			

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: limited username, limited password, full username, full password, read-only community strings, read/ write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Check Point FireWall-1, Solaris, version NG

FEATURE	CLI	SNMP
Driver Discovery	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table	X	
OSPF Neighbors		
Interfaces	X	
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		X
ICMP Test	X	
Topology Parsing	X	
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management (can modify: limited username, limited password, full username, full password)	X	
Syslog Configuration and Change Detection		

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Check Point FireWall-1, Nokia, version NG

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table	X	
OSPF Neighbors		
Interfaces	X	
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		X
ICMP Test	X	
Topology Parsing	X	
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management		
Syslog Configuration and Change Detection		

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Check Point Provider 1, Linux, version NG

FEATURE	CLI	TFTP/CLI
Driver Discovery	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)		X
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table	X	
OSPF Neighbors		
Interfaces		
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		
ICMP Test	X	
Topology Parsing	X	
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management (can modify: limited password, full username, full password)	X	
Syslog Configuration and Change Detection		

FEATURE	CLI	TFTP/CLI
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Check Point SecurePlatform, Linux, version NG

FEATURE	CLI	SNMP
Driver Discovery	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table	X	
OSPF Neighbors		
Interfaces	X	
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		X
ICMP Test	X	
Topology Parsing	X	
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management (can modify: limited username, limited password, full username, full password)	X	
Syslog Configuration and Change Detection		

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Known Issues

objects.C and rules.C Configuration Files

If the Check Point device is managed by a Check Point management engine, it is unnecessary for NCM to capture the objects.C and rules.C configuration files for this device. Instead, configure the Check Point management engine within NCM with the access variable “checkpointManagementEngine”. This will force NCM to capture the global objects.C and rules.C from the Check Point management engine. The data is mostly redundant, as the Check Point management engine submits the information to all of the nodes for which it is responsible.

Ciena CN 2000 Storage Extension Platform, OS version 4.x

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table	X	
OSPF Neighbors		
Interfaces	X	
Modules and Inventory	X	
Flash Storage Space		
File System		
Uptime		
ICMP Test	X	
Topology Parsing		
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management		

FEATURE	CLI	SNMP
Syslog Configuration and Change Detection	X	
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Cisco ACE Application Control Engine Module, version 3.0

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP	CLI
Driver Discovery	X	X			
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X		X	X	X
Configuration					
Configuration Snapshot (Startup configuration captured: yes)			X		X
Device information parsing (supported)					
Enhanced Layer2 Basic IP information parsing (supported)					
Configuration Deployment (destinations: to running, to startup with reboot)			X		
Diagnostics					
Routing Table	X				
OSPF Neighbors					
Interfaces	X				
Modules and Inventory					
Flash Storage Space					
File System	X				
Uptime		X			
ICMP Test	X				
Topology Parsing	X				
Duplex Mismatch Parsing	X				
Other					

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP	CLI
Software Center	X				
Password Management (can modify: limited password, read-only community strings)	X				
Syslog Configuration and Change Detection					
Custom Scripts and Diagnostics	X				
ACL Management					
Configlet Parsing					

Cisco Aironet access points 340 & 350 series, VXWorks Software

FEATURE	CLI	SNMP	TFTP/SNMP
Driver Discovery		X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)		X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)			X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment			X
Diagnostics			
Routing Table			
OSPF Neighbors			
Interfaces		X	
Modules and Inventory			
Flash Storage Space			
File System			
Uptime		X	
ICMP Test			
Topology Parsing			
Duplex Mismatch Parsing	X		
Other			
Software Center			X

FEATURE	CLI	SNMP	TFTP/SNMP
Password Management			
Syslog Configuration and Change Detection		X	
Custom Scripts and Diagnostics			
ACL Management			
Configlet Parsing			

Known Issues

Real-time change detection via Syslog is limited

The ability to detect a configuration change via Syslog is limited to looking for a reload message. No other Syslog messages from the device will indicate the possibility of a configuration change. This means that, effectively, real-time change detection via Syslog is not supported.

Custom diagnostics not supported

The driver performs custom scripting by deploying a script to the device via TFTP. This method of scripting is incompatible with the custom diagnostics feature. Therefore, although the driver will allow for the creation of custom scripts, it will not allow for the creation of custom diagnostics.

Workaround:

Use a custom script to perform diagnostics. This will not result in captured diagnostic data being stored. You will need to review the results of the command script task instead.

Cisco Aironet access points, 350, 1100, 1200 & 1300 series, IOS version 12.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X		X	X
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destinations: to running, to startup with reboot)			X	X
Diagnostics				
Routing Table				
OSPF Neighbors				
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing	X			
Other				

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Software Center	X			
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Known Issue

Listing of image files during a software update

The Update Device Software task enables you to update a device's OS software. When performing a software update, the FileSystem diagnostic provides a list of image files. This enables you to select image files for removal before you run the Update Device Software task. When upgrading the Aironet C1310, the checkbox settings for the image files are ignored due to limited support in the driver. Other Aironet devices should not be affected by this issue.

Cisco Wide Area Application Engine WAE-7300 Series (ACNS) 5.3.3

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X		
Configuration			
Configuration Snapshot (Startup configuration captured: yes)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to running, to startup with reboot)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces			
Modules and Inventory	X		
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing	X		
Other			

FEATURE	CLI	SNMP	TFTP/CLI
Software Center			
Password Management (can modify: full password, read-only community strings, read/ write community strings)	X		
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Cisco Application and Content Networking System Software (ACNS) version 5.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X		
Configuration			
Configuration Snapshot (Startup configuration captured: yes)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to running, to startup with reboot)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces			
Modules and Inventory	X		
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing	X		
Other			

FEATURE	CLI	SNMP	TFTP/CLI
Software Center			
Password Management (can modify: full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Cisco Global Site Selector (GSS), OS version 1.2

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: SSH1, SSH2, Console)	X	
Configuration		
Configuration Snapshot (Startup configuration captured: yes)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table	X	
OSPF Neighbors		
Interfaces	X	
Modules and Inventory		
Flash Storage Space		
File System	X	
Uptime		X
ICMP Test	X	
Topology Parsing	X	
Duplex Mismatch Parsing	X	
Other		
Software Center		
Password Management		
Syslog Configuration and Change Detection	X	

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics	X	
ACL Management	X	
Configlet Parsing		

Known Issue

Difference between Startup and Running Configurations

NCM gathers a two-part configuration for this device:

1. Running configuration
2. Results of ‛show tech-support config.’

NCM also gathers a Startup configuration. Because NCM compares the Startup configuration to the two-block unit above, it will always show a difference. However, if the comparison of startup-to-running shows differences in the “tech-support” block only, the Startup configuration and the Running configuration are in sync.

Cisco Hubs, 1548 series, Version 1.0.0

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table		
OSPF Neighbors		
Interfaces	X	
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		
ICMP Test	X	
Topology Parsing		
Duplex Mismatch Parsing	X	
Other		
Software Center		
Password Management (can modify: full password, read-only community strings, read/write community strings)	X	
Syslog Configuration and Change Detection		

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Cisco FastHub 400 series, OS version 1.0

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, Console)	X	
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table		
OSPF Neighbors		
Interfaces	X	
Modules and Inventory		
Flash Storage Space		
File System		
Uptime	X	
ICMP Test		
Topology Parsing		
Duplex Mismatch Parsing		
Other		
Software Center	X	
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X	

FEATURE	CLI	SNMP
Syslog Configuration and Change Detection		
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Cisco IGX/BPX/MGX

FEATURE	CLI	SNMP
Driver Discovery		X
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table	X	
OSPF Neighbors		
Interfaces		
Modules and Inventory	X	
Flash Storage Space		
File System		
Uptime		X
ICMP Test		
Topology Parsing	X	
Duplex Mismatch Parsing	X	
Other		
Software Center		
Password Management (can modify: full username, full password, read-only community strings, read/write community strings)	X	
Syslog Configuration and Change Detection		

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Cisco load-balancers, CSS 11000 series (Arrowpoint)

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X		X	
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destination: to running)			X	
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System				
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing	X			
Other				
Software Center				

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Password Management (can modify: limited username, limited password, full username, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management				
Configlet Parsing				

Known Issues

Configuration commands can be reformatted and shuffled during deployment

After you deploy a configuration, it is common for the CSS to shuffle or change the format of commands in the configuration file. Afterwards, it appears that numerous lines were added, removed, or modified when comparing configurations. You must inspect the configuration manually to determine which commands were moved and which were actually changed by the deploy task.

Cisco switches, 1900 Series, OS version 9.x Standard Edition

FEATURE	CLI	SNMP
Driver Discovery	X	
General Access (CLI protocols: Telnet Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment (destination: to running)		
Diagnostics		
Routing Table		
OSPF Neighbors		
Interfaces	X	
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		
ICMP Test	X	
Topology Parsing		
Duplex Mismatch Parsing	X	
Other		
Software Center	X	

FEATURE	CLI	SNMP
Password Management (can modify: limited password)	X	
Syslog Configuration and Change Detection		
Custom Scripts and Diagnostics		
ACL Management		
Configlet Parsing		

Known Issues

Driver Support

When using SNMP to discover a Cisco 1900 Standard Edition device, NCM could inadvertently assign the Cisco 1900 Enterprise Edition driver to the device. To correct this, either use the CLI to discover the device or manually assign the Cisco 1900 Standard Edition driver to the device.

Cisco switches, Catalyst 2820, 2900, 4000, 5000, 6000 & 7606 series, hybrid mode, Catalyst OS

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing	X		
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Known Issues

Deploy configuration reports error, but actually succeeds

When deploying a configuration to a device running CatOS, the device provides error messages that may or may not signify an error in the deployed configuration. The task completes as Failed even if the deployment was successful. You should review the warning messages provides in the task results to determine whether they are benign or not.

Note: *You can determine whether the deployment task was successful by clicking the "Compare to Previous Configuration" link and confirming that the configuration changes are as expected.*

CatOS versions prior to 5.5 do not support change detection via Syslog

CatOS versions prior to 5.5 do not support Syslog configuration change messaging.

Cisco switches, Catalyst 4000 & 6000 series, native mode, Modular IOS version 12.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP	SCP/CLI	SCP/SNMP
Driver Discovery	X	X				
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X	X	X
Configuration						
Configuration Snapshot (Startup configuration captured: yes)	X		X	X		
Device information parsing (supported)						
Enhanced Layer2 Basic IP information parsing (supported)						
Configuration Deployment (destinations: to running, to startup with reboot)						
Diagnostics						
Routing Table	X					
OSPF Neighbors	X					
Interfaces	X					
Modules and Inventory						
Flash Storage Space						
File System	X					

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP	SCP/CLI	SCP/SNMP
Uptime		X				
ICMP Test	X					
Topology Parsing	X					
Duplex Mismatch Parsing						
Other						
Software Center	X					
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X					
Syslog Configuration and Change Detection	X					
Custom Scripts and Diagnostics	X					
ACL Management	X					
Configlet Parsing						

Known Issue

Software Center: Patch deployment only

Currently, Software Center for this driver only supports the installation of patches. Base software modularity images cannot be applied through NCM. As a result, they will have to be manually installed.

Cisco switches, Catalyst Blade Switch (CBS) 30x0 series, IOS version 12.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP	SCP/CLI	SCP/SNMP
Driver Discovery	X	X				
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X	X	X
Configuration						
Configuration Snapshot (Startup configuration captured: yes)			X	X	X	
Device information parsing (supported)						
Enhanced Layer2 Basic IP information parsing (supported)						
Configuration Deployment						
Diagnostics						
Routing Table	X					
OSPF Neighbors	X					
Interfaces	X					
Modules and Inventory						
Flash Storage Space						
File System	X					
Uptime		X				
ICMP Test	X					

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP	SCP/CLI	SCP/SNMP
Topology Parsing	X					
Duplex Mismatch Parsing						
Other						
Software Center						
Password Management						
Syslog Configuration and Change Detection						
Custom Scripts and Diagnostics						
ACL Management	X					
Configlet Parsing						

Cisco routers, 800, 1700, 2500, 2600, 4000, 4500 & 4700 series, IOS version 12.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X		X	X
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destinations: to running, to startup with reboot)			X	X
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing	X			
Other				

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Software Center	X			
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Known Issues

Default IOS prompts expected

NCM expects the default prompts for Cisco IOS devices and cannot discover or otherwise interact with the device if it is unable to recognize the following device prompts:

- Exec: >
- Enable: #
- Config:)#

If your organization routinely uses non-standard IOS device prompts, contact Customer Support to see whether NCM can be reconfigured to match your environment.

SNMP/TFTP Configuration Deployment task may time-out

Cisco devices with slower processors may time-out an SNMP/TFTP Configuration Deployment task.

Workaround:

Deploy configurations via CLI/TFTP only.

ACL remarks will get duplicated on deployment

Cisco devices can maintain multiple lines of “remarks” for access list specifications. The device does not check for duplication of remark lines. Any deployment of a remark back to the running configuration of the device will create another remark line (a duplicate).

Workaround:

Use NCM persistent comments for ACL remarks. This capability is handled automatically by using ACL comments in NCM.

Routing Table diagnostic shows BGP summary if BGP enabled

If BGP is enabled, the Routing Table diagnostic will provide the results of the “show ip bgp summary” command. This prevents NCM from requesting and storing a routing table that is likely to be extraordinarily large and time-consuming to capture.

During Software Update task, the Delete Files action may not succeed if image filenames are non-standard

During a Software Image Update task, NCM attempts to upload a new software image with the same filename as the existing image. Some IOS versions do not support this. Choosing the “Delete files option from selected slot” option, compact memory can support the image update by deleting the existing file before attempting to upload the new image. However, this action succeeds only if the existing image uses the default *.bin* filename extension.

If the image file has been renamed using a non-default extension, NCM cannot find or delete the file and the new image cannot be uploaded. The Device Software Update task will fail. In these cases use a different image filename. Alternatively, you can prepare the flash manually or via a custom command script before deploying the software image.

Note: *The Delete Files operation deletes only .bin file extensions to prevent any configuration or crash information files in flash memory from being deleted.*

Software Center functionality is not supported on Cisco 2500 routers

If you attempt to deploy software against a 2500 router, you may see the success messages listed below. However, the software is not updated and the device may be placed in an inaccessible state. Also, it may no longer have a boot image to load.

1. Snapshot task preceding software update result: succeeded View Result
2. Prepare memory script result: succeeded View Result
3. Software update script for c2500-i-1.121-21.bin result: succeeded
4. Discovery task following software update result: succeeded

Remark lines are replicated when access list is redeployed

Cisco IOS devices enable users to enter more than one remark line per access list. When this access list is redeployed, the device replicates each remark line.

Workaround:

Use the NCM commenting feature to create and track configuration comments.

Cisco IOS XR, CRS, and compatible GSR routers

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X			
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destinations: to running, to startup with reboot)			X	X
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System				
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing	X			
Other				

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Software Center				
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Cisco ONS 15454, OS version 5.4, 6.02.02

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table		
OSPF Neighbors		
Interfaces		
Modules and Inventory	X	
Flash Storage Space		
File System		
Uptime		X
ICMP Test		
Topology Parsing		
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management		
Syslog Configuration and Change Detection		

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Known Issue

Cisco ONS limited functionality

The Cisco ONS driver is limited in functionality due to:

- The complex configurations that are possible given the many Network Interface Cards (NICs) that can be installed.
- The limited availability of a fully, or typically, configured chassis with provisioned NICs, facilities, services, circuits, tunnels, and so on.
- The usual manner for configuring and managing the device is via a proprietary GUI.

NMAP network device detection not supported

The NMAP network device detection function is not supported for Cisco ONS 15454 devices running OS versions 5.x or 6.x. NMAP detects a generic signature which cannot be mapped to a particular device class.

Cisco Routers, 1700, 2500, 2600 & 4700 series, IOS version 11.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X		X	X
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destinations: to running, to startup with reboot)			X	X
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing	X			
Other				

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Software Center				
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Known Issues

Default IOS prompts expected

NCM expects the default prompts for Cisco IOS devices and cannot discover or otherwise interact with the device if it is unable to recognize the following prompts:

- Exec: >
- Enable: #
- Config:)#

If your organization routinely uses non-standard IOS device prompts, contact Customer Support to see if NCM can be reconfigured to match your environment.

Remark lines are replicated when access list is redeployed

Some Cisco IOS devices enable users to enter more than one remark line per access list. When this access list is redeployed, the device replicates each remark line.

Workaround:

Use the NCM commenting feature to create and track configuration comments.

Cisco switches, Catalyst 5000 RSM & 6000 MSFC routing module, hybrid mode, IOS version 12.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X		X	X
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destinations: to running, to startup with reboot)			X	X
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing	X			
Other				

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Software Center	X			
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Known Issues

Default IOS prompts expected

NCM expects the default prompts for Cisco IOS devices and cannot discover or otherwise interact with the device if it is unable to recognize the following prompts:

- Exec: >
- Enable: #
- Config:)#

If your organization routinely uses non-standard IOS device prompts, contact Customer Support to see if NCM can be reconfigured to match your environment.

SNMP/TFTP Configuration Deployment task may time out

Cisco devices with slower processors may time out an SNMP/TFTP Configuration Deployment task.

Workaround:

Deploy configurations via CLI/TFTP only.

ACL remarks will get duplicated on deployment

Cisco devices can maintain multiple lines of remarks for access list specifications. The device does not check for duplication of remark lines. Consequently, any deployment of a remark back to the running configuration of the device will create another remark line (a duplicate).

Workaround:

Use NCM persistent comments for ACL remarks. This capability is handled automatically by using ACL comments in NCM.

During Software Update task, the Delete Files action may not succeed if image filenames are non-standard

During a Software Image Update task, NCM attempts to upload a new software image with the same filename as the existing image. Some IOS versions do not support this action. Choosing the Delete files from selected slot option, compact memory can support the image update by deleting the existing file before attempting to upload the new image. However, this action succeeds only if the existing image uses the default filename extension .bin.

If the image file has been renamed using a non-default extension, NCM cannot find or delete the file and the new image cannot be uploaded. The Device Software Update task will fail. In these cases use a different image filename. Alternatively, you can prepare the flash manually or via a custom command script before deploying the software image.

Note: *The Delete Files operation deletes only .bin file extensions to prevent any configuration or crash information files in flash memory from being deleted.*

Remark lines are replicated when access list is redeployed

Some Cisco IOS devices enable users to enter more than one remark line per access list. When this access list is redeployed, the device replicates each remark line.

Workaround:

Use the NCM commenting feature to create and track configuration comments.

Cisco switches, Catalyst 5000 RSM & 6000 MSFC routing module, hybrid mode, IOS version 11.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X		X	X
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment			X	X
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing	X			
Other				

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Software Center	X			
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Cisco routers, 12000 series (GSR), IOS version 12.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X		X	X
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destinations: to running, to startup with reboot)			X	X
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing	X			
Other				
Software Center	X			

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Known Issues

Default IOS prompts expected

NCM expects the default prompts for Cisco IOS devices and cannot discover or otherwise interact with the device if it is unable to recognize the following device prompts:

- Exec: >
- Enable: #
- Config:)#

If your organization routinely uses non-standard IOS device prompts, contact Customer Support to see if NCM can be reconfigured to match your environment.

SNMP/TFTP Configuration Deployment task may time out

Cisco devices with slower processors may time out an SNMP/TFTP Configuration Deployment task.

Workaround:

Deploy configurations via CLI/TFTP only.

ACL remarks will get duplicated on deployment

Cisco devices can maintain multiple lines of remarks for access list specifications. The device does not check for duplication of remark lines. Consequently, any deployment of a remark back to the running configuration of the device will create another remark line (a duplicate).

Workaround:

Use NCM persistent comments for ACL remarks. This capability is handled automatically by using ACL comments in NCM.

During the Software Update task, the Delete Files action may not succeed if image filenames are non-standard

During a Software Image Update task, NCM attempts to upload a new software image with the same filename as the existing image. Some IOS versions do not support this task. Choosing the Delete files from selected slot option, compact memory can support the image update by deleting the existing file before attempting to upload the new image. However, this action succeeds only if the existing image uses the default filename extension .bin.

If the image file has been renamed using a non-default extension, NCM cannot find or delete the file and the new image cannot be uploaded. The Device Software Update task will fail. In these cases use a different image filename. Alternatively, you can prepare the flash manually or via a custom command script before deploying the software image.

Note: *The Delete Files task deletes only .bin file extensions to prevent any configuration or crash information files in flash memory from being deleted.*

Remark lines are replicated when access list is redeployed

Some Cisco IOS devices enable users to enter more than one remark line per access list. When this access list is redeployed, the device replicates each remark line.

Workaround:

Use the NCM commenting feature to create and track configuration comments.

Cisco routers, 7200 & 7500 series, IOS version 12.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X		X	X
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment			X	X
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing	X			
Other				
Software Center	X			

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Known Issues

Default IOS prompts expected

NCM expects the default prompts for Cisco IOS devices and cannot discover or otherwise interact with the device if it is unable to recognize the following device prompts:

- Exec: >
- Enable: #
- Config:)#

If your organization routinely uses non-standard IOS device prompts, contact Customer Support to see if NCM can be reconfigured to match your environment.

SNMP/TFTP Configuration Deployment task may time out

Cisco devices with slower processors may time out an SNMP/TFTP Configuration Deployment task.

Workaround:

Deploy configurations via CLI/TFTP only.

ACL remarks will get duplicated on deployment

Cisco devices can maintain multiple lines of remarks for access list specifications. The device does not check for duplication of remark lines. Consequently, any deployment of a remark back to the running configuration of the device will create another remark line (a duplicate).

Workaround:

Use NCM persistent comments for ACL remarks. This capability is handled automatically by using ACL comments in NCM.

During the Software Update task, the Delete Files action may not succeed if image filenames are non-standard

During a Software Image Update task, NCM attempts to upload a new software image with the same filename as the existing image. Some IOS versions do not support this task. Choosing the Delete files from selected slot option, compact memory can support the image update by deleting the existing file before attempting to upload the new image. However, this action succeeds only if the existing image uses the default filename extension .bin.

If the image file has been renamed using a non-default extension, NCM cannot find or delete the file and the new image cannot be uploaded. The Device Software Update task will fail. In these cases use a different image filename. Alternatively, you can prepare the flash manually or via a custom command script before deploying the software image.

Note: *The Delete Files task deletes only .bin file extensions to prevent any configuration or crash information files in flash memory from being deleted.*

Remark lines are replicated when access list is redeployed

Some Cisco IOS devices enable users to enter more than one remark line per access list. When this access list is redeployed, the device replicates each remark line.

Workaround:

Use the NCM commenting feature to create and track configuration comments.

Cisco routers, 7200 & 7500 series, IOS version 11.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X		X	X
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destinations: to running, to startup with reboot)			X	X
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing	X			
Other				
Software Center	X			

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Cisco switches, Catalyst 4000, 6000 & 7600 series, native mode, IOS version 12.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X		X	X
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment			X	X
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces				
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing	X			
Other				

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Software Center	X			
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Known Issues

Default IOS prompts expected

NCM expects the default prompts for Cisco IOS devices and cannot discover or otherwise interact with the device if it is unable to recognize the following device prompts:

- Exec: >
- Enable: #
- Config:)#

If your organization routinely uses non-standard IOS device prompts, contact Customer Support to see if NCM can be reconfigured to match your environment.

SNMP/TFTP Configuration Deployment task may time out

Cisco devices with slower processors may time out an SNMP/TFTP Configuration Deployment task.

Workaround:

Deploy configurations via CLI/TFTP only.

ACL remarks will get duplicated on deployment

Cisco devices can maintain multiple lines of remarks for access list specifications. The device does not check for duplication of remark lines. Consequently, any deployment of a remark back to the running configuration of the device will create another remark line (a duplicate).

Workaround:

Use NCM persistent comments for ACL remarks. This capability is handled automatically by using ACL comments in NCM.

During the Software Update task, the Delete Files action may not succeed if image filenames are non-standard

During a Software Image Update task, NCM attempts to upload a new software image with the same filename as the existing image. Some IOS versions do not support this task. Choosing the Delete files from selected slot option, compact memory can support the image update by deleting the existing file before attempting to upload the new image. However, this action succeeds only if the existing image uses the default filename extension .bin.

If the image file has been renamed using a non-default extension, NCM cannot find or delete the file and the new image cannot be uploaded. The Device Software Update task will fail. In these cases use a different image filename. Alternatively, you can prepare the flash manually or via a custom command script before deploying the software image.

Note: *The Delete Files task deletes only .bin file extensions to prevent any configuration or crash information files in flash memory from being deleted.*

Remark lines are replicated when access list is redeployed

Some Cisco IOS devices enable users to enter more than one remark line per access list. When this access list is redeployed, the device replicates each remark line.

Workaround:

Use the NCM commenting feature to create and track configuration comments.

Cisco switches, Catalyst 4000 & 6000 series, native mode, IOS version 11.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X		X	X
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destinations: to running, to startup with reboot)			X	X
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces				
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing	X			
Other				

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Software Center	X			
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Known Issues

Catalyst 4000 series (Native Mode): Deploy Configuration not supported for older IOS versions

On the Catalyst 4000 Series, NCM uses the CISCO-CONFIG-COPY-MIB to deploy configuration files via SNMP. IOS 11.x and early IOS 12.0/12.1 releases do not support this MIB. Therefore, configuration deployment is not supported on these older OS versions.

When the MIB is not supported, you will see the following error message:

```
The system could not deploy this config - Execution step resulted
in total bypass. Check the connections methods supported by the
device.
```

To deploy configurations on the Catalyst 4000 through SNMP, you must upgrade to IOS 12.1(11b)EW or later.

Cisco routers, 3600 & MC3810 series, IOS version 12.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X		X	X
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment			X	X
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing	X			
Other				
Software Center	X			

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Known Issues

Default IOS prompts expected

NCM expects the default prompts for Cisco IOS devices and cannot discover or otherwise interact with the device if it is unable to recognize the following device prompts:

- Exec: >
- Enable: #
- Config:)#

If your organization routinely uses non-standard IOS device prompts, contact Customer Support to see if NCM can be reconfigured to match your environment.

SNMP/TFTP Configuration Deployment task may time out

Cisco devices with slower processors may time out an SNMP/TFTP Configuration Deployment task.

Workaround:

Deploy configurations via CLI/TFTP only.

ACL remarks will get duplicated on deployment

Cisco devices can maintain multiple lines of remarks for access list specifications. The device does not check for duplication of remark lines. Consequently, any deployment of a remark back to the running configuration of the device will create another remark line (a duplicate).

Workaround:

Use NCM persistent comments for ACL remarks. This capability is handled automatically by using ACL comments in NCM.

During the Software Update task, the Delete Files action may not succeed if image filenames are non-standard

During a Software Image Update task, NCM attempts to upload a new software image with the same filename as the existing image. Some IOS versions do not support this task. Choosing the Delete files from selected slot option, compact memory can support the image update by deleting the existing file before attempting to upload the new image. However, this action succeeds only if the existing image uses the default filename extension .bin.

If the image file has been renamed using a non-default extension, NCM cannot find or delete the file and the new image cannot be uploaded. The Device Software Update task will fail. In these cases use a different image filename. Alternatively, you can prepare the flash manually or via a custom command script before deploying the software image.

Note: *The Delete Files task deletes only .bin file extensions to prevent any configuration or crash information files in flash memory from being deleted.*

Remark lines are replicated when access list is redeployed

Some Cisco IOS devices enable users to enter more than one remark line per access list. When this access list is redeployed, the device replicates each remark line.

Workaround:

Use the NCM commenting feature to create and track configuration comments.

Cisco routers, 3600 series, IOS version 11.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X		X	X
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment			X	X
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing	X			
Other				
Software Center				

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Cisco switches, Catalyst 2950, 2948G, 2950, 2950T, 3550, 3750 & 8500 series, IOS version 12.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X		X	X
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment			X	X
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing	X			
Other				

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Software Center	X			
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Known Issues

Default IOS prompts expected

NCM expects the default prompts for Cisco IOS devices and cannot discover or otherwise interact with the device if it is unable to recognize the following device prompts:

- Exec: >
- Enable: #
- Config:)#

If your organization routinely uses non-standard IOS device prompts, contact Customer Support to see if NCM can be reconfigured to match your environment.

Catalyst 3550: Cannot take snapshots using SNMP

The Catalyst 3550 does not support the standard Cisco MIB CISCO-CONFIG-COPY. Therefore, it cannot support SNMP for snapshots. However, discovery can still occur using SNMP.

SNMP/TFTP Configuration Deployment task may time out

Cisco devices with slower processors may time out an SNMP/TFTP Configuration Deployment task.

Workaround:

Deploy configurations via CLI/TFTP only.

ACL remarks will get duplicated on deployment

Cisco devices can maintain multiple lines of remarks for access list specifications. The device does not check for duplication of remark lines. Consequently, any deployment of a remark back to the running configuration of the device will create another remark line (a duplicate).

Workaround:

Use NCM persistent comments for ACL remarks. This capability is handled automatically by using ACL comments in NCM.

During the Software Update task, the Delete Files action may not succeed if image filenames are non-standard

During a Software Image Update task, NCM attempts to upload a new software image with the same filename as the existing image. Some IOS versions do not support this task. Choosing the Delete files from selected slot option, compact memory can support the image update by deleting the existing file before attempting to upload the new image. However, this action succeeds only if the existing image uses the default filename extension .bin.

If the image file has been renamed using a non-default extension, NCM cannot find or delete the file and the new image cannot be uploaded. The Device Software Update task will fail. In these cases use a different image filename. Alternatively, you can prepare the flash manually or via a custom command script before deploying the software image.

Note: *The Delete Files task deletes only .bin file extensions to prevent any configuration or crash information files in flash memory from being deleted.*

Remark lines are replicated when access list is redeployed

Some Cisco IOS devices enable users to enter more than one remark line per access list. When this access list is redeployed, the device replicates each remark line.

Workaround:

Use the NCM commenting feature to create and track configuration comments.

Updating the Cisco 3750 in a master/slave configuration

When updating the Cisco 3750 in a master/slave configuration, the software image must be deployed to each Cisco 3750 in the stack. This is usually done by deploying to *flash:, flash1:, flash2:,* and so on. To set the OS image, select “OS” on *flash:* only.

Cisco switches, Catalyst 2900XL, 3500XL & 4908G-L3 series, IOS version 12.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X		X	X
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment			X	X
Diagnostics				
Routing Table				
OSPF Neighbors				
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing	X			
Other				
Software Center	X			

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Cisco switches, Catalyst 2900XL, 3500XL, 4908G-L3 & GESM series, IOS version 12.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP	CLI
Driver Discovery	X	X			
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X	X
Configuration					
Configuration Snapshot (Startup configuration captured: yes)			X	X	X
Device information parsing (supported)					
Enhanced Layer2 Basic IP information parsing (supported)					
Configuration Deployment (destination: to running, to startup with reboot)			X	X	
Diagnostics					
Routing Table					
OSPF Neighbors					
Interfaces	X				
Modules and Inventory	X				
Flash Storage Space					
File System	X				
Uptime					
ICMP Test	X				
Topology Parsing	X				
Duplex Mismatch Parsing	X				

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP	CLI
Other					
Software Center	X				
Password Management (can modify: limited password, full password, read-only community strings, read/ write community strings)	X				
Syslog Configuration and Change Detection	X				
Custom Scripts and Diagnostics	X				
ACL Management	X				
Configlet Parsing					

Cisco switches, Catalyst 2900XL & 3500XL series, IOS version 11.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X		X	X
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destination: to running)			X	X
Diagnostics				
Routing Table				
OSPF Neighbors				
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing	X			
Other				

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Software Center				
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Cisco switches, Catalyst 1900 series, OS version 9.x.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X		X	
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X		X	X
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destination: to running)			X	
Diagnostics				
Routing Table				
OSPF Neighbors				
Interfaces	X			
Modules and Inventory				
Flash Storage Space				
File System				
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing	X			
Other				
Software Center	X			

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection				
Custom Scripts and Diagnostics	X			
ACL Management				
Configlet Parsing				

Known Issues

Catalyst 1900: Does not support Syslog change detection

The Catalyst 1900 does not send Syslog messages.

Cisco SAN switches, 9000 series, SAN-OS version 2.x(2b)

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP	CLI
Driver Discovery	X	X			
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X		X	X	X
Configuration					
Configuration Snapshot (Startup configuration captured: yes)			X		X
Device information parsing (supported)					
Enhanced Layer2 Basic IP information parsing (supported)					
Configuration Deployment (destination: to running, to startup with reboot))			X		
Diagnostics					
Routing Table	X				
OSPF Neighbors					
Interfaces	X				
Modules and Inventory	X				
Flash Storage Space					
File System	X				
Uptime					
ICMP Test	X				
Topology Parsing	X				
Duplex Mismatch Parsing	X				

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP	CLI
Other					
Software Center	X				
Password Management (can modify: limited password, read-only community strings, read/ write community strings)	X				
Syslog Configuration and Change Detection	X				
Custom Scripts and Diagnostics	X				
ACL Management					
Configlet Parsing					

Known Issue

Updating Device Software

During an Update Device Software task on a Cisco SAN switch, the driver replaces the files used for "kickstart" and "system." As a result, you must reboot the device so that these files can be used.

When attempting to downgrade software on a Cisco SAN switch, only one of the "Fabric" modules (in a redundant scenario) is downgraded. In addition, the downgrade sets the "Fabric" module with the highest OS version as active. This could cause the device to use an incorrect OS version or become inaccessible if the active "Fabric" module is not configured correctly.

Configuration retrieval on SAN-OS version 2.x

Configuration retrieval via TFTP has been disabled on SAN-ON version 2.x devices becasue extraneous configuration data could appear when retrieving a configuration via TFTP.

Cisco routers, IOS, unrecognized model number or IOS version

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X		X	X
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment				
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing	X			
Other				
Software Center				

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Password Management				
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management (ACL parsing only)				
Configlet Parsing				

Known Issues

Default IOS prompts expected

NCM expects the default prompts for Cisco IOS devices and cannot discover or otherwise interact with the device if it is unable to recognize the following device prompts:

- Exec: >
- Enable: #
- Config:)#

If your organization routinely uses non-standard IOS device prompts, contact Customer Support to see if NCM can be reconfigured to match your environment.

Cisco firewalls, ASA 5500 series, OS version 7.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access			
Configuration			
Configuration Snapshot (Startup configuration captured: yes)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to running, to startup with reboot)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System	X		
Uptime			
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing	X		
Other			
Software Center	X		
Password Management (can modify: limited password, full password, read-only community strings)	X		

FEATURE	CLI	SNMP	TFTP/CLI
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics (bulk deploy available)	X		
ACL Management	X		
Configlet Parsing			

Cisco firewalls, Firewall Services Module (FWSM) Series

FEATURE	CLI	TFTP/CLI
Driver Discovery	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: yes)	X	X
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment (destinations: to running, to startup with reboot)		X
Diagnostics		
Routing Table	X	
OSPF Neighbors	X	
Interfaces	X	
Modules and Inventory		
Flash Storage Space		
File System	X	
Uptime		
ICMP Test	X	
Topology Parsing	X	
Duplex Mismatch Parsing	X	
Other		

FEATURE	CLI	TFTP/CLI
Software Center	X	
Password Management (can modify: limited password, full password, read-only community strings)	X	
Syslog Configuration and Change Detection	X	
Custom Scripts and Diagnostics	X	
ACL Management	X	
Configlet Parsing		

Cisco firewalls, Firewall Services Module (FWSM) Series, Context within Multiple Mode

FEATURE	CLI	TFTP/CLI
Driver Discovery	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: yes)	X	X
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment (destination: to running)		X
Diagnostics		
Routing Table	X	
OSPF Neighbors	X	
Interfaces	X	
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		
ICMP Test	X	
Topology Parsing	X	
Duplex Mismatch Parsing	X	
Other		

FEATURE	CLI	TFTP/CLI
Software Center		
Password Management (can modify: limited password, full password, read-only community strings)	X	
Syslog Configuration and Change Detection	X	
Custom Scripts and Diagnostics	X	
ACL Management	X	
Configlet Parsing		

Cisco firewalls, PIX series

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	
Configuration				
Configuration Snapshot (Startup configuration captured: no)			X	
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destination: to running)			X	
Diagnostics				
Routing Table	X			
OSPF Neighbors				
Interfaces	X			
Modules and Inventory				
Flash Storage Space				
File System				
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing	X			
Other				
Software Center	X			

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Password Management (can modify: limited password, full password, read-only community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Known Issues

Changing the TFTP interface access setting

To retrieve (or deploy) a PIX device configuration using TFTP, you may need to specify the TFTP interface to use on the device. If the device self-selects the wrong interface for the TFTP settings, you can override the TFTP interface access setting in the device's password rules in NCM. Keep in mind that you must either set up a device-specific password rule or define a password rule that applies specifically to PIX devices that are exhibiting this problem.

To change a device password rule:

1. Edit the device and select “Use device-specific password information” or create or edit a device password rule applying to the appropriate device(s).
2. Click “Show Device Access Settings.”
3. Choose “PIX TFTP interface” from one of the drop-down menus for “Name.”
4. Enter the desired interface (for example “outside”) for the “Value” of this setting.
5. Ensure all other authentication information is correct and save the device or password rule.

Double-check deployed configurations

The PIX occasionally has difficulty merging new configuration commands with the existing configuration. Because of this, you should double-check PIX configurations after you deploy them from NCM.

1. Take a snapshot of the configuration.
2. Check if your changes were deployed to the running configuration as expected. Sometimes NCM reports the deployment as failed, but still applies changes to the running configuration.

No support for real-time change detection via AAA

The PIX does not support accounting sessions. Therefore, NCM cannot provide real-time change detection through AAA.

Cisco firewalls, PIX series (no TFTP)

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery				
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	
Configuration				
Configuration Snapshot (Startup configuration captured: no)	X			
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment				
Diagnostics				
Routing Table	X			
OSPF Neighbors				
Interfaces	X			
Modules and Inventory				
Flash Storage Space				
File System				
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing	X			
Other				
Software Center	X			

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Password Management (can modify: limited password, full password, read-only community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Known Issues

No support for real-time change detection via AAA

The PIX does not support accounting sessions. Therefore, NCM cannot provide real-time change detection through AAA.

Cisco firewalls, PIX series, 7.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X		X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running, to startup with reboot)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System	X		
Uptime			
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing	X		
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify limited password, full password, read-only community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Cisco firewalls, Riverhead Guard, OS version 3.x

FEATURE	CLI	SNMP
Driver Discovery	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table		
OSPF Neighbors		
Interfaces	X	
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		X
ICMP Test		
Topology Parsing	X	
Duplex Mismatch Parsing	X	
Other		
Software Center		
Password Management		
Syslog Configuration and Change Detection	X	

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Cisco load balancers, LD series

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	
Configuration				
Configuration Snapshot (Startup configuration captured: no)	X		X	
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destination: to running)			X	
Diagnostics				
Routing Table	X			
OSPF Neighbors				
Interfaces	X			
Modules and Inventory				
Flash Storage Space				
File System				
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing	X			
Other				
Software Center	X			

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Password Management (can modify: limited password, full password, read-only community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Cisco Voice Gateway VG248, OS version 1.x

FEATURE	CLI	SNMP
Driver Discovery	X	
General Access (CLI protocols: Telnet, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment (destination: to running)		
Diagnostics		
Routing Table		
OSPF Neighbors		
Interfaces		
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		X
ICMP Test	X	
Topology Parsing		
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X	

FEATURE	CLI	SNMP
Syslog Configuration and Change Detection		
Custom Scripts and Diagnostics		
ACL Management		
Configlet Parsing		

Cisco VPN Products, VPN 3000 series, OS version 3.x and higher

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	
Configuration				
Configuration Snapshot (Startup configuration captured: no)	X		X	
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destination: to running)			X	
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory				
Flash Storage Space				
File System				
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing	X			
Other				
Software Center	X			

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Password Management (can modify: limited password, full password, read-only community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics				
ACL Management				
Configlet Parsing				

Cisco WAE Products, WAE611/WAE612 Wide Area Application Services (WAAS), OS version 4.x and higher

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: yes)			X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to running, to startup with reboot)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime			
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing	X		

FEATURE	CLI	SNMP	TFTP/CLI
Other			
Software Center			
Password Management (can modify limited username, limited password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management (ALC parsing only)	X		
Configlet Parsing			

Cisco 2006, 4400 Wireless LAN Controller

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment			
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System			
Uptime			
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing	X		
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify limited username, limited password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management (ALC parsing only)	X		
Configlet Parsing			

Known Issue

Read/Write community strings

Read/write community strings are masked by the Cisco 4400 Wireless LAN device. As a result, NCM cannot parse that information.

Citrix NetScaler 9000 Series Switch, 6.x

FEATURE	CLI	SNMP	FTP/CLI
Driver Discovery	X	X	
General Access (CLI protocol: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: yes)			
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to running, to startup with reboot)			
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center	X		

FEATURE	CLI	SNMP	FTP/CLI
Password Management (can modify full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Colubris MAP-320/330, OS version 5.1.3

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to running)	X		
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center			

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify full username, full password, read-only community strings, and read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management (ALC parsing only)			
Configlet Parsing			

Comtech 5650 Satellite modem, OS version 1.04.02

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table		
OSPF Neighbors		
Interfaces		
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		X
ICMP Test		
Topology Parsing		
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management		
Syslog Configuration and Change Detection		

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics		
ACL Management (ALC parsing only)		
Configlet Parsing		

Crossbeam Security Services Switch, C-Series, COS 3.0.1-15

FEATURE	CLI	SNMP
Driver Discovery	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment	X	
Diagnostics		
Routing Table	X	
OSPF Neighbors		
Interfaces	X	
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		X
ICMP Test	X	
Topology Parsing	X	
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management		
Syslog Configuration and Change Detection		

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics		
ACL Management		
Configlet Parsing		

Cyberguard Firewalls, FS 300/600, KS 1000/1500

FEATURE	CLI	SNMP
Driver Discovery	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment (destinations: to running)	X	
Diagnostics		
Routing Table	X	
OSPF Neighbors		
Interfaces	X	
Modules and Inventory		
Flash Storage Space		
File System	X	
Uptime	X	
ICMP Test	X	
Topology Parsing	X	
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management		
Syslog Configuration and Change Detection		

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics	X	
ACL Management (ALC parsing only)		
Configlet Parsing		

Known Issues

General Access: Connection is only possible through a bastion host

Some versions of SSH on the Cyberguard device (FSecure-SSH 2.0.x) include a bug in the key exchange code that breaks SSH communication. Although there is a workaround used by many SSH clients, the current version of NCM does not include these workarounds.

Workaround: Use an SSH relay host (referred to as a bastion host) if the SSH client on the bastion host contains the workaround. NCM can communicate with the Cyberguard device through this relay channel. Bastion host requirements include:

- A Windows or Linux server running a recent version of openssh.
- A non-privileged account username/password.

NCM must be able to reach the bastion host via the network. In turn, the bastion host must be able to reach the Cyberguard device.

1. Login to NCM.
2. On the NCM menu bar under devices, click Inventory.
3. Locate the Cyberguard device (if you already added it) and click the Edit option in the Actions column.
4. If you have not added the Cyberguard device, add the device in NCM and set it up with the correct username, password, and other settings.
5. On the Edit Device page, scroll down to the Connection Information section and check the “Connect with bastion host” checkbox.
6. Enter the hostname/IP of the bastion host, along with the username/ password of the un-privileged account.
7. Click the Save Device button.

8. Connect to the device.

The recommended bastion host setup is with a Linux system running a recent distribution with openssh packages installed

The Cyberguard device supports both Telnet and SSH. However, the device supports only root access via a non-privileged login followed by a “setlvl” command and then “su”. The latter two steps are only allowed when using SSH connections for security reasons. Therefore, although the driver supports Telnet, it cannot be used for accessing the device's configuration if the included files are root-read-only.

Configuration Deployment

The Cyberguard device is a Unix system running firewall software. This driver supports the gathering of the firewall’s configuration file, as well as information about the system, including hostname, routing table, and so on. Configuration deployment is supported, but only for the firewall’s configuration files. Other system data gathered from command outputs cannot be deployed back to the device.

Cyclades Terminal Servers, Device Series, OS version 1.3.x

FEATURE	CLI	SNMP	SCP/CLI
Driver Discovery	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)			
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment	X		
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center			X

FEATURE	CLI	SNMP	SCP/CLI
Password Management (can modify: full username, full password)	X		
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management (ACL parsing only)			
Configlet Parsing			

Cyclades Terminal Servers, Device Series, OS version 1.4.x

FEATURE	CLI	SNMP	SCP/CLI
Driver Discovery	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)			
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment	X		
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			

FEATURE	CLI	SNMP	SCP/CLI
Software Center			X
Password Management (can modify: full username, full password)	X		
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management (ACL parsing only)			
Configlet Parsing			

Cyclades Terminal Servers, Device Series, OS version 2.6.x

FEATURE	CLI	SNMP	SCP/CLI
Driver Discovery	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X		X
Configuration			
Configuration Snapshot (Startup configuration captured: no)			
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to running)	X		
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System	X		
Uptime	X		
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			

FEATURE	CLI	SNMP	SCP/CLI
Software Center			X
Password Management (can modify: full password)	X		
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management (ACL parsing only)			
Configlet Parsing			

Dell PowerConnect 3248 Switch, OS version 1.x, 2.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocol: Telnet, console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: yes)	X		
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to startup with reboot)			X
Diagnostics			
Routing Table			
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test			
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify limited username, limited password, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Known Issue

Minimal syslog support

The Dell PowerConnect 3248 can be configured for Syslog notification via NCM. However, the device limits functonality to warm start notifications. Snapshots will not be triggered via Syslog for this device.

SSH support

The Dell PowerConnect 3248 running OS version 2.0.0.21 supports SSH1 access only. However, if the device is running version 1.x opdcode, SSH access is not supported.

Password length

The Dell PowerConnect 3248 limits password length to eight characters. Attempting to deploy passwords longer than eight characters will fail and the original password will remain in effect.

Configuration deployment

The Dell PowerConnect 3248 can use TFTP to deploy to running or startup. However, NCM cannot determine success or failure of the transfer to running. As a result, it is not supported in the driver. Configuration deployment to startup or startup with reload is supported.

Dell PowerConnect 3448P Switch, OS version 1.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocol: Telnet, console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: yes)	X		
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to running, to startup with reboot)			X
Diagnostics			
Routing Table			
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System	X		
Uptime			
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify limited password, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Dell PowerConnect 6248 Switch, OS version 1.x, 2.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocol: Telnet, console)	X		X
Configuration			
Configuration Snapshot (Startup configuration captured: yes)	X		
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to startup with reboot)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center			

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (limited username, limited password, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Known Issue

Device Access Levels

The Dell PowerConnect 6248 switch enables you to add users with varying access levels. When deploying a new user, NCM does not determine the access level of the pre-existing user. Instead, NCM adds the new user with an access level of 1 and sets the enable password to the current device access rule or device settings.

Digi PortServer TS 8/16 MEI, TS 16 Rack

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocol: Telnet, ssh2, console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to running, to startup with reboot)	X		
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces			
Modules and Inventory			
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Known Issues

Digi PortServers TS access user

To access the Digi PortServers TS, NCM must use the “root” user.

Digi PortServers TS access prompts

The “root” prompt must end with the default characters (#>). Failure to do so prevents NCM from properly accessing the device. The “root” prompt can be set to the default values by issuing the following command:

```
set netlogin rootprompt = #>
```

Digi PortServers TS CLI prompts

Login and Password prompts should be set to the default values when connecting via Telnet (in the case of SSH failure or when SSH is disabled on the device). The default prompts can be set by issuing the following commands:

```
set netlogin passprompt = password:
set netlogin logprompt = login:
```

Digi PortServers TS configuration CLI deployment

Configuration lines longer than 132 characters are not accepted by the Digi PortServers TS device and will generate a Warning when being deployed via the CLI.

Digi PortServers TS configuration TFTP deployment

TFTP deployment could fail with the “Host stopped responding” error message.

Digi PortServers TS community strings

The Digi PortServer TS 8/16 MEI, TS 16 Rack driver cannot delete the Read-Write community string on the device. NCM returns an error message if you attempt to deploy a null or blank, or null value. Because the value for the Write community string is hidden in the device configuration, NCM always displays it as `*****` on the password deployment page. You can always see the community strings that were last deployed on the Edit Device page, under the device-specific password information tab.

Digi PortServers TS filesystem

Because there is no way to obtain the total and free amount of memory on the Digi Portserver, NCM sets both values to 0.

Edgewater Edgemarc, Device Series 4200, 4300, 4500 and 5300, OS version 6.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocol: Telnet, console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to startup with reboot)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime			
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center			

FEATURE	CLI	SNMP	TFTP/CLI
Password Management			
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Enterasys Matrix switches, V2H Series, OS version 2.2.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X		X	
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destination: to startup with reboot)			X	
Diagnostics				
Routing Table				
OSPF Neighbors				
Interfaces	X			
Modules and Inventory				
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing				
Other				

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Software Center	X			
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Enterasys Matrix switches, SecureStack C2 Series, OS version 3.0x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running)	X		
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			

FEATURE	CLI	SNMP	TFTP/CLI
Software Center	X		
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Known Issues

Active software images cannot be deleted

If a software image is "Active" on the device, it cannot be deleted. An attempt to delete an active image will cause the task to fail.

Workaround:

Deploy a new image first. Once the device has reloaded and accepted the new image, delete the old image in a new task.

Setting the boot image will reboot the device

When an new image is added to the device and the system is instructed to use the image to boot the device, the device will reload.

Workaround:

Only update the image when it is acceptable for the device to reload.

Enterasys Matrix switches and routers, SecureStack C2 Series, OS version 4.0.x, 5.0.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, Console)	X		X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running)	X		
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Known Issues

SSH protocol error

SSH returns a protocol error through our SSH library. As a result, SSH cannot be used to connect to the Enterasys Matrix device.

Terminal length value

The device configuration supports virtually any positive integer value for terminal length. However, the suggested value should be greater than 25 as the device could potentially lock up with smaller values. The terminal length is set by default to 50, and can be modified from the 'prompt_length' variable.

Configuration deployment requirements

Configuration are deployed line-by-line using the CLI session. However, the Enterasys Matrix device could ignore configuration options that are part of its configuration set. If this occurs, the deployment task could fail.

Workaround:

Use the Edit & Deploy option to minimize the amount of configuration options being uploaded to the device. If possible, only change a subset of the configuration instead of deploying the entire configuration.

Configuration deployment with a Radius server

When deploying a configuration containing a Radius server, the Enterasys Matrix device might prompt you to provide the Radius server secret.

Workaround:

Set the custom device access setting *radius_secret* to add the desired Radius server secret. If this variable is not set, the task will fail.

CLI deployment

CLI deployment is used because TFTP deployment results in the Enterasys Matrix device rewriting the default configuration (a 15k file) over the deployed non-default configuration (3k).

Syslog server usage

The Enterasys Matrix device requires a Syslog server index be used to identify a Syslog server. As a result, NCM must utilize an index in the server table. NCM will default to using the 8th slot.

Workaround:

If this occurs, set the *syslogIndex* variable to another number.

ACLs types

The Enterasys Matrix device could contain policy rules that are configurable in the Enable mode and access lists managed from Router mode. When editing a policy rule, the driver must be in Enable mode. As a result, three “exit” commands are required in the ACL script.

Enterasys XP-8000 SmartSwitch Router 8 (SSR-8) Router, OS version 9.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: yes)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to startup with reboot)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System	X		
Uptime			
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			

FEATURE	CLI	SNMP	TFTP/CLI
Software Center			
Password Management (can modify: limited password, full password)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Known Issues

SSHv2 protocol error

SSHv2 returns a protocol error through the NCM SSH Library. As a result, SSH cannot be used to connect to the Enterasys XP-8000 SmartSwitch router.

Proxy sessions

Proxy sessions to the Enterasys XP-8000 SmartSwitch router could take a few minutes to close after you have disconnected from the device.

Pre-task snapshots

There could be issues with tasks that require a pre-task snapshot being unable to re-login to the Enterasys XP-8000 SmartSwitch router. It is recommended that you retry the tasks or contact Support for assistance.

Expand Routers, Accelerator Series, OS version 4.5

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)			
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to startup with reboot)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Extreme switches, Summit series

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	
Configuration				
Configuration Snapshot (Startup configuration captured: no)	X		X	
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destination: to startup with reboot)			X	
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing				
Other				
Software Center	X			

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Password Management (can modify: limited username, limited password, full username, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Known Issues

Ping results vary in number of attempts

Extreme devices run the Ping test until manually cancelled. NCM handles this by initiating the Ping test, waiting five seconds, then interrupting the Ping test and capturing the results. A typical Ping test shows the results of between two and eight cycles.

Configuration commands shuffled and reformatted during deployment

After you deploy a configuration, it is common for Extreme devices to shuffle or change the format of commands in the configuration file. Afterwards, it appears that numerous lines were added, removed, or modified when comparing configurations. You must inspect the configuration manually to determine which commands were moved and which were actually changed by the deploy task.

Ensure two blank lines follow banner when deploying configuration

Extreme devices support multi-line banners. Two blank lines following a banner definition indicate that the banner is complete. If there are less than two blank lines following the banner, the Extreme device will interpret the remainder of the configuration as part of the banner. It is important to ensure that these blank lines are always in the correct place and not to insert in-line comments in a manner that might disrupt this.

Extreme Summit 200 and 400 series do not support hardware information diagnostic

The Extreme Summit 200 and 400 series devices do not support the commands used by the hardware information diagnostic. Attempts to run this diagnostic against these devices will result in a failure.

Changing user name via Password Management will delete previous account

The limited access username and password in “Password Management” relates to a “user” account on Extreme devices. Similarly, the full access username and password relates to an “admin” account. If you change the name of either of these accounts, the existing account will be deleted to ensure that old usernames do not remain on the device as a “back door”.

Extreme Summit maintains default community strings unless explicitly overridden

The Extreme Summit always defaults to a read-only community string of “public” and a read/write community string of “private”. These values are accepted by the device unless you explicitly define other values for the read-only and read/write community strings. If you delete your community string values, the defaults are automatically restored.

Extreme switches, Summit series, SummitStack, Software version XOS 11.6, 12.0

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, Console)	X		X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running)	X		
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test			
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: full username, full password, read-only community strings, read/ write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Known Issues

Updating Device Software

During the software update process, if a software image is uploaded to an active partition on an Extreme switch, the Update Device Software task will reboot the device even if the "Reboot device after deploying software" option is unchecked. As a result, if you upload software to a device with more than one software image in the same Update Device Software task, the task will fail.

SSH not supported

The Extreme XOS can be enhanced with a module to support SSH2. However, responses to SSH2 connections are not always the same. As a result, SSH2 connections fail 70% of the time. Because of this inconsistent behavior, SSH is not Supported on Extreme switches.

Using the same name for different ACLs results in incorrect ACL content

Although Extreme switches permit two, different ACLs with the same name, the driver cannot make the distinction between them. As a result, if two different ACLs share the same name, the information for both ACLs is parsed as a single ACL.

NCM will not delete ACL zones unless there are no ACLs using the ACL zone

Deleting an ACL zone requires the deletion of all ACLs that use that zone. The driver will only delete an ACL zone if all ACLs using that zone have been removed.

Software updates

During software updates, some commands are executed after a delay, while others are not executed at all or return errors. The CLI should not be used during software updates.

New software images overwrite previous software images

Newly uploaded software images will overwrite previous software images from the memory slot on which they were uploaded.

Extreme switches, Black Diamond Series

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	
Configuration				
Configuration Snapshot (Startup configuration captured: no)	X		X	
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment			X	
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing				
Other				
Software Center	X			

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Password Management (can modify: limited username, limited password, full username, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Known Issues

Transition from TFTP to CLI snapshot may shuffle commands

The Extreme Black Diamond may report spurious configuration changes due to shuffling command order if NCM transitions from capturing the configuration via TFTP to capturing it via CLI (such as in the event of a TFTP failure).

Configuration commands shuffled and reformatted during deployment

After you deploy a configuration, it is common for Extreme devices to shuffle or change the format of commands in the configuration file. Afterwards, it appears that numerous lines were added, removed, or modified when comparing configurations. You must inspect the configuration manually to determine which commands were moved and which were actually changed by the deploy task.

Ensure two blank lines follow banner when deploying configuration

Extreme devices support multi-line banners. Two blank lines following a banner definition indicate that the banner is complete. If there are less than two blank lines following the banner, the Extreme will interpret the remainder of the configuration as part of the banner. It is important to ensure that these blank lines are always in the correct place and not to insert in-line comments in a manner that might disrupt this.

Ping results vary in number of attempts

Extreme devices run the Ping test until manually cancelled. NCM handles this by initiating the Ping test, waiting five seconds, then interrupting the Ping test and capturing the results. A typical Ping test shows the results of between two and eight cycles.

Password Management of community strings will leave old strings on device

When editing SNMP community strings through “Password Management” on the Extreme Black Diamond, the new strings will be added. However, the old strings will not be deleted on the device.

Extreme switches, Black Diamond 10000 series

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (to running)	X		
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System	X		
Uptime			
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: limited username, limited password, full username, full password, read-only community strings, read/write community strings)			
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Extreme switches, Alpine Series

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	
Configuration				
Configuration Snapshot (Startup configuration captured: no)	X		X	
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment			X	
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing				
Other				
Software Center	X			

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Password Management (can modify: limited username, limited password, full username, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Known Issues

Configuration commands shuffled and reformatted during deployment

After you deploy a configuration, it is common for Extreme devices to shuffle or change the format of commands in the configuration file. Afterwards, it appears that numerous lines were added, removed, or modified when comparing configurations. You must inspect the configuration manually to determine which commands were moved and which were actually changed by the deploy task.

Ensure two blank lines follow banner when deploying configuration

Extreme devices support multi-line banners. Two blank lines following a banner definition indicate that the banner is complete. If there are less than two blank lines following the banner, the Extreme will interpret the remainder of the configuration as part of the banner. It is important to ensure that these blank lines are always in the correct place and not to insert in-line comments in a manner that might disrupt this.

Ping results vary in number of attempts

Extreme devices run the Ping test until manually cancelled. NCM handles this by initiating the Ping test, waiting five seconds, then interrupting the Ping test and capturing the results. A typical Ping test shows the results of between two and eight cycles.

Extreme switches, 200 & 400 Series

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	
Configuration				
Configuration Snapshot (Startup configuration captured: no)	X		X	
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment			X	
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory				
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing				
Other				
Software Center	X			

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Password Management (can modify: limited username, limited password, full username, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

F5 (multi-config) load-balancers, Big-IP series, OS version 4.x

FEATURE	CLI	SNMP	SCP/CLI
Driver Discovery	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)			X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center			

FEATURE	CLI	SNMP	SCP/CLI
Password Management (can modify: full username, full password)	X		
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management (ACL parsing only)	X		
Configlet Parsing			

Known Issues

Running custom action scripts

If you run a custom action script that modifies the F5 device configuration, be sure to add the appropriate command to save the modified configuration(s). This might include syncing the configurations with neighboring F5 devices that are setup to share the same configuration options.

Telnet access commonly disabled

By default, the Big-IP does not support Telnet connections. Consequently, when NCM attempts to access the device using Telnet it will fail. It is recommended that you disable Telnet as a protocol for these devices to avoid unnecessary failures.

Use Edit & Deploy to modify community strings

Community string management is not supported by NCM Password Management. However, you can use Edit & Deploy to modify device community strings if necessary.

Use integrated SSH, console port, or F5 GUI to ensure real-time change detection

For real-time change detection, it is recommended that you use the NCM integrated SSH client, the console port, or the device's graphical user interface (GUI). Otherwise, NCM may not detect configuration changes.

F5 (multi-config) load-balancers, 3-DNS series, OS version 4.x

FEATURE	CLI	SNMP	SCP/CLI
Driver Discovery	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment	X		
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center			

FEATURE	CLI	SNMP	SCP/CLI
Password Management (can modify: full username, full password)	X		
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Known Issues

Running custom action scripts

If you run a custom action script that modifies the F5 device configuration, be sure to add the appropriate command to save the modified configuration(s). This might include syncing the configurations with neighboring F5 devices that are setup to share the same configuration options.

Telnet access commonly disabled

By default, the Big-IP does not support Telnet connections. Consequently, when NCM attempts to access the device using Telnet it will fail. It is recommended that you disable Telnet as a protocol for these devices to avoid unnecessary failures.

Use Edit & Deploy to modify community strings

Community string management is not supported by NCM Password Management. However, you can use Edit & Deploy to modify device community strings if necessary.

Use integrated SSH, console port, or F5 GUI to ensure real-time change detection

For real-time change detection, it is recommended that you use the NCM integrated SSH client, the console port, or the device's graphical user interface (GUI). Otherwise, NCM may not detect configuration changes.

F5 (multi-config) load-balancers, Big-IP series, OS version 9.x

FEATURE	CLI	SNMP	SCP/CLI
Driver Discovery	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment			
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center			

FEATURE	CLI	SNMP	SCP/CLI
Password Management (can modify: full username, full password)	X		
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Known Issues

Running custom action scripts

If you run a custom action script that modifies the F5 device configuration, be sure to add the appropriate command to save the modified configuration(s). This might include syncing the configurations with neighboring F5 devices that are setup to share the same configuration options.

Telnet access commonly disabled

By default, the Big-IP does not support Telnet connections. Consequently, when NCM attempts to access the device using Telnet it will fail. It is recommended that you disable Telnet as a protocol for these devices to avoid unnecessary failures.

Use Edit & Deploy to modify community strings

Community string management is not supported by NCM Password Management. However, you can use Edit & Deploy to modify device community strings if necessary.

Use integrated SSH, console port, or F5 GUI to ensure real-time change detection

For real-time change detection, it is recommended that you use the NCM integrated SSH client, the console port, or the device's graphical user interface (GUI). Otherwise, NCM may not detect configuration changes.

Force10 Networks routers, E Series, OS version 5.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X		X	
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destinations: to running, to startup with reboot)			X	
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing				
Other				
Software Center	X			

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Password Management (limited password, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management				
Configlet Parsing				

Fore Systems Hub asx1000, OS Version 5.x

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment	X	
Diagnostics		
Routing Table	X	
OSPF Neighbors		
Interfaces	X	
Modules and Inventory	X	
Flash Storage Space		
File System	X	
Uptime		
ICMP Test	X	
Topology Parsing		
Duplex Mismatch Parsing		
Other		
Software Center	X	
Password Management (limited username, limited password, full password, read-only community strings, read/write community strings)	X	

FEATURE	CLI	SNMP
Syslog Configuration and Change Detection	X	
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Fortinet Fortigate-60M Antivirus Firewall, OS version 3.00

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X			
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: no)			X	
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destination to running)			X	
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory				
Flash Storage Space				
File System				
Uptime				
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing				
Other				

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Software Center	X			
Password Management (full username, full password, read-only community strings)	X			
Syslog Configuration and Change Detection				
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Known Issues

Fortinet Fortigate-60M does not support Syslog change detection

The Fortinet Fortgate-60M does not send Syslog messages for Admin login/ logoff or configuration changes.

Foundry routers, Software version 07.1.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: yes)	X		X	X
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destinations: to running, to startup with reboot)			X	X
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory				
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing				
Other				
Software Center	X			

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Known Issues

Configuration setting required for proper snapshots

You must include the “enable password display” command in the configuration of Foundry devices to ensure that snapshots and polling work correctly.

Configuration deployment through SNMP

When deploying configurations to Foundry devices through SNMP, you must:

- Include the “no snmp-server pw-check” command.
- Not use the “snmp-client <ip>” command or use the IP address of the NCM server.

Software upload may fail due to TFTP server timeout

An attempt to upload software to a Foundry device via TFTP may fail. During a TFTP transfer, the Foundry performs various memory cleanup operations that require additional processing time. The TFTP server times-out if the server's timeout property value is set too low. The default value is 3000 milliseconds (3 seconds). When this error occurs, the following message is displayed on the Task Details page: `Script - Failed`

Although the task shows as failed, the software may have been successfully uploaded. However, the reboot process fails. You can eliminate this problem by setting the value of the timeout property in the “tftpd.properties” file to a higher value.

To set the TFTP server timeout property:

1. On the Windows NCM server, go to *C:\Rendition\server\ext\tftp*.
2. Using a text editor, such as Notepad, open the *tftpd.properties* file.
3. Edit the “TFTP timeout socketTimeout” property to a value between 5000 and 10000 (5 to 10 seconds).

Funkwerk Artem W3002T, OS version 6.05

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table	X	
OSPF Neighbors		
Interfaces	X	
Modules and Inventory	X	
Flash Storage Space		
File System		
Uptime		
ICMP Test		
Topology Parsing	X	
Duplex Mismatch Parsing		
Other		
Software Center		

FEATURE	CLI	SNMP
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X	
Syslog Configuration and Change Detection	X	
Custom Scripts and Diagnostics		
ACL Management	X	
Configlet Parsing		

HP Procurve switches, M Series, OS version 08.x, 09.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to startup with reboot)			X
Diagnostics			
Routing Table			
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: limited password, full password)	X		
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Known Issues

Unable to store proxy session logs

NCM is unable to parse the session logs from a ProCurve proxy session. Therefore, proxy session logs are not stored for the ProCurve.

Device can become unresponsive is accessed with SSHv2

When an attempt is made to connect to a ProCurve device via SSHv2, the device can become unresponsive ("hang") and not return a valid response. If you see this occurring, you should disable SSHv2 in NCM.

Deployment can fail due to slow TFTP retrieval

The Procurve may not download its configuration file as fast as NCM expects it to. Consequently, the configuration file is removed from the TFTP server directory before the device has completed loading it. This will cause the TFTP process to fail and the deployed changes will not appear on the device. You can override the "tftpDelay" Device Access Setting (default is 10 seconds) and set a higher value if necessary.

HP ProCurve switches, 2500 Series, OS version F.05.x and 5308xl, OS version E.08.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: yes)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to startup with reboot)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			

FEATURE	CLI	SNMP	TFTP/CLI
Software Center	X		
Password Management (can modify: limited username, limited password, full username, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Known Issue

Device discovery via SSH/Telnet on 5308xl devices configured without passwords is unreliable

On HP Procurve 5308xl devices configured without password authentication, SSH/Telnet device discovery could occasionally fail due to the inconsistent display of the signon banner page.

For reliable device discovery via SSH/Telnet, passwords should be set for the Operator or Manager access accounts on HP Procurve 5308xl devices.

HP Procurve switches, 2600 Series, OS version 7.x, 8x. 10x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: yes)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment			X
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: limited username, limited password, full username, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing	X		

Known Issue

Modifying the hostname on HP ProCurve 26xx devices

The default exec and enable prompt on HP ProCurve switches include the ">" and "#" as ending characters, respectively. Although the hostname of HP ProCurve switches can contain these characters, they should be omitted because NCM could potentially get out of sync during task processing.

HP Procurve switches, 3500, 5406 Series, OS versions 11.x, 12.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: yes)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running, startup with reboot)	X		
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			

FEATURE	CLI	SNMP	TFTP/CLI
Software Center	X		
Password Management (can modify: limited username, limited password, full username, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Known Issue

Device authentication failures

By default, user names and passwords sent to the HP Procurve device are masked from the authentication logs when using NCM 1.x or later. If you encounter authentication failures:

1. Login to NCM.
2. On the menu bar, select Devices and click Inventory.
3. On the Inventory page, locate the HP Procure device.
4. In the Actions column, click the Edit option.
5. On the Edit Device page, scroll down to the Device Access Settings field.
6. Change the Custom Setting to: `send_slow`
7. Change the Value to: `true`
8. Click the Save Device button.

Keep in mind that after the *send_slow* variable is set to true, the authentication logs will contain user names and passwords in clear text.

HP ProLiant switches, OS version 2.0

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running)			X
Diagnostics			
Routing Table			
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime			
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: full username, full password, read-only community strings, read/ write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Huawei Quidway AR 28-31 Router, OS version 3.4

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: yes)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to startup with reboot)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: can modify: limited username, limited password, full username, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Huawei Quidway NetEngine and ARxx series routers, H3C S3xxx, S5xxx and S7xxx series switches, OS versions 3.x, 5.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: yes)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to startup with reboot)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			

FEATURE	CLI	SNMP	TFTP/CLI
Other			
Software Center	X		
Password Management (can modify: limited username, limited password, full username, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Intel Sarvega Guardian Gateway, XESOS version 5.1.x

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: yes)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table	X	
OSPF Neighbors		
Interfaces	X	
Modules and Inventory	X	
Flash Storage Space		
File System		
Uptime		
ICMP Test	X	
Topology Parsing		
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management (can modify full username and full password, read-only community strings)	X	
Syslog Configuration and Change Detection		

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Juniper CTP 2000 series Application Switches, OS version 4.1R11

FEATURE	CLI	SNMP	SCP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to running)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			

FEATURE	CLI	SNMP	SCP/CLI
Software Center			
Password Management			
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Juniper (Perbit) WXC-500, WX-100; OS Version 5.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery		X	
General Access (CLI protocols: SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: yes)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to running)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System	X		
Uptime			
ICMP Test	X		
Topology Parsing			
Duplex Mismatch Parsing			
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: limited username, limited password, full username, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Juniper routers, OS version 5.5, 6.x, 7.x, 8.x

FEATURE	CLI	SNMP	TFTP/CLI	SCP/CLI
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: no)	X		X	
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destinations: to running to startup with reboot)				X
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing				
Other				
Software Center	X			X

FEATURE	CLI	SNMP	TFTP/CLI	SCP/CLI
Password Management (can modify: full username, full password, read-only community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Known Issues

Snapshot fails using SSHv1 or Telnet

NCM’s current implementation of SCP only supports SSHv2 as a connection method. Using SCP with SSHv1 or Telnet is not supported.

Bulk configuration deployment

The JunOS operating system stores its configuration in a hierarchical structure rather than as a series of commands. Bulk configuration deployment is designed to handle the merging of configuration data blocks directly, while line-by-line deployment is designed to run a series of commands.

SNMP Discovery

You can edit the SysDescr SNMP value on Juniper devices. However, not including the OS version SysDescr value makes SNMP-only discovery fail.

Software Center

The JunOS operating system requires certain characters be escaped with a leading backslash (\) in the filenames for files deployed to Juniper routers. NCM does not support the use of the backslash (\) character when deploying a Software Update Image or when deleting files from the device using the Sync Image option on the Image Synchronization Report.

In fact, there are additional characters with special meaning to NCM that should not be used:

- Opening square bracket ([ )
- Opening round bracket and the closing round bracket (( )).
- Caret (^)
- Dollar sign ($)
- Period or dot (.)
- Vertical bar or pipe symbol (|)
- Question mark (?)
- Asterisk or star (*)
- Plus sign (+)

JunOS SCP library incompatibility

Software Center operations could experience protocol errors due to issues with SCP library compatibility with JunOS version 8.1R3.3.

Juniper (Redline) E|X DeviceType, 3650 Series, OS version 5.0

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery		X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to running)			X
Diagnostics			
Routing Table			
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center			

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: full username, full password, read-only community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Known Issues

Invalid configurations could be due to TFTP failures

The Juniper (Redline) does not report failure conditions when exporting a configuration via TFTP. If the device is reporting invalid configurations, this could be due to unreported TFTP failures by the device.

Workaround:

Capture the session log of a snapshot and look for the “export” commands being run on the device. Check to see if the specified TFTP server in the command is correct. If it is correct, you might need to manually debug TFTP transfers from the device to the NCM server. Alternately, you can edit the device and disable TFTP. The configuration will be captured directly from the CLI session.

Juniper Voiceflow Session Border Controller, Series 3000, OS version 5.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: yes)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to startup with reboot)	X		
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime			
ICMP Test	X		
Topology Parsing			
Duplex Mismatch Parsing			
Other			

FEATURE	CLI	SNMP	TFTP/CLI
Software Center			
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Juniper Voiceflow Session Border Controller, Series 3000, OS version 6.x and above

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: yes)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to startup with reboot)	X		
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime			
ICMP Test	X		
Topology Parsing			
Duplex Mismatch Parsing			
Other			

FEATURE	CLI	SNMP	TFTP/CLI
Software Center			
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Juniper (formerly NetScreen) firewalls & VPNs, OS version 2.6.1, 5.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: full username, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Known Issues

NCM may fail to connect if maximum logins are exceeded

Juniper (formerly) NetScreen devices allow a maximum of three terminal sessions. If NCM tries to login when the maximum number of sessions are already established, NCM will fail to login to the device. All tasks requiring CLI access, including snapshost, password changes, and configuration deployments, will fail in this case.

Certain configuration commands cannot be used in deployment

Juniper (formerly NetScreen) devices do not accept certain commands when deploying configurations to the device. For example, the device does not allow you to modify the “set admin sys-location” command via Deploy Configuration. In addition, NetScreen devices occasionally have difficulty merging new configuration commands with the existing configuration. Cisco recommends that you verify the NetScreen configuration after you deploy it from NCM.

To verify that your changes were correctly deployed to the running configuration, use the “Compare to Previous” link provided in the task details of a successful Deploy Configuration task.

SSH v1 and SSH v2 support

On Juniper (formerly NetScreen) devices, you can enable either SSH v1 and SSH v2, but not simultaneously.

SSH connection could fail if additional command is set

On Juniper (formerly) NetScreen devices, it is possible to turn off "SSH Password Authentication" for a user. To disable this feature, enter the *set admin scs password enable username $user* CLI command (where *$user* is the username). By default, this option is not enabled.

Lantronix Ethernet Terminal Servers, ETS8P/ETS16P, OS version V3.x/x

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: yes)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment	X	
Diagnostics		
Routing Table		
OSPF Neighbors		
Interfaces	X	
Modules and Inventory		
Flash Storage Space		
File System	X	
Uptime		X
ICMP Test	X	
Topology Parsing		
Duplex Mismatch Parsing		
Other		
Software Center	X	

FEATURE	CLI	SNMP
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X	
Syslog Configuration and Change Detection		
Custom Scripts and Diagnostics	X	
ACL Management	X	
Configlet Parsing		

Known Issue

Access prompts

The non-privileged mode access prompt for the Lantronix ETS must end with the right angle bracket character (`>`). This character cannot be used elsewhere in the prompt.

The privileged mode access prompt flag `%P` must be set to `%P>` to denote the privileged user, for example: `Local_%n%P>`. Failure to do so will prevent NCM from properly accessing the device. The privileged mode access prompt is set as follows: `SET/DEFINE SERVER PROMPT PromptString>%P`.

Lucent MAX 6000 Router, OS version 7.x.x

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, Console)	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: no)			X	
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment			X	X
Diagnostics				
Routing Table	X			
OSPF Neighbors				
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime				
ICMP Test				
Topology Parsing				
Duplex Mismatch Parsing				
Other				
Software Center				
Password Management				

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Syslog Configuration and Change Detection				
Custom Scripts and Diagnostics	X			
ACL Management				
Configlet Parsing				

Known Issue

Post-Task Snapshots

When scheduling tasks on a Lucent MAX 6000 router that require a post-task snapshot, NCM could have a problem re-logging into the device to perform the post-task snapshot. It is recommended that you retry the tasks or contact Customer Support for assistance.

Maipu 1762, 2700, 3000 series routers, OS version 3.x and 5.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: yes)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to startup with reboot)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			

FEATURE	CLI	SNMP	TFTP/CLI
Software Center	X		
Password Management (can modify: limited username, limited password, full username, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Marconi switches, Fore series

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to running and to startup with reboot)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center			

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: limited username, limited password, full username, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Known Issues

Authentication failures may result from too many open sessions

Prior to version 8.0, the Marconi Fore OS supported only one session per device (after 8.0 it allows two). If the maximum number of sessions are already established, any subsequent attempt to connect to the device will result in a failure to connect. This failure will appear in NCM as an authentication error. In fact, however, the authentication information used by NCM may be acceptable, but the device does not have any sessions available.

Deployment to running configuration may not apply all configuration changes

Some configuration commands on Marconi Fore devices will not take effect until after a reboot. Therefore, attempts to deploy to the device's running configuration may not apply all desired changes to the configuration. You should use the “Deploy to startup config and reboot” option to deploy configurations if you think there is a chance some of the commands you are deploying may not take effect without a reboot.

Motorola (MoCa) PathBuilder 2500, 4000, 6000 Series, OS version 11.x, 14.x, 15.x

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: SSH2, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table	X	
OSPF Neighbors	X	
Interfaces	X	
Modules and Inventory	X	
Flash Storage Space		
File System	X	
Uptime		
ICMP Test	X	
Topology Parsing		
Duplex Mismatch Parsing		
Other		
Software Center	X	

FEATURE	CLI	SNMP
Password Management (can modify full username and full password)		
Syslog Configuration and Change Detection	X	
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Known Issue

boot.cfg file

During normal operation, changes to the Motorola (MoCa) PathBuilder device's running configuration, either by NCM or normal user access, are saved to the boot.cfg file that is loaded on device reboot. When the device reboots, any changes made that have not been added to the boot.cfg file are lost. When Deploy-to-Startup is engaged, only changes included in the boot.cfg file being deployed will be seen after the device reboots.

NEC IX5000 Series Switch, OS version 7.x and higher

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment (destinations: to running)	X	
Diagnostics		
Routing Table	X	
OSPF Neighbors	X	
Interfaces	X	
Modules and Inventory	X	
Flash Storage Space		
File System	X	
Uptime		
ICMP Test	X	
Topology Parsing	X	
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management (can modify: limited username, limited password, full password, read-only community strings, read/write community strings)	X	

FEATURE	CLI	SNMP
Syslog Configuration and Change Detection	X	
Custom Scripts and Diagnostics	X	
ACL Management	X	
Configlet Parsing		

NEC Univerge 2000 Series Routers, OS version 5.x, 7.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to startup with reboot)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime			
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center			

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: full username, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Known Issues

NEC IX2000 Devices running 5.x code do not support SYSLOG

There is no logging subsystem support for configuration change detection under 5.x code, even though the option is available. (Note: No harm is caused by attempting to configure SYSLOG. It simply does not function.)

NEC IX2000 devices can be slow to recover from discovery Telnet sessions

On NEC IX2000 devices, tasks scheduled to run automatically after device discovery could fail due to an inability to immediately reconnect to the device. While these tasks can be restarted manually, they could recover on their own.

NEC IX2000 devices do not contain domain name information

On NEC IX2000 devices, name servers are defined within BasicIP for client agents. However, the device exists without domain information.

NET Scream 50/100, OS version X

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table		
OSPF Neighbors		
Interfaces	X	
Modules and Inventory	X	
Flash Storage Space		
File System		
Uptime		X
ICMP Test	X	
Topology Parsing		
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management		
Syslog Configuration and Change Detection		

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Network Appliance Proxy, NetCache Series, OS version 5.5x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment			
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System			
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			

FEATURE	CLI	SNMP	TFTP/CLI
Software Center			
Password Management (can modify: full password)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Network Appliance Proxy, NetCache Series, OS version 7.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, Console)	X		X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment			
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System			
Uptime			
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center			

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: full password)	X		
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Known Issue

Use of SSH for device access is not supported

The Network Appliance Proxy, NetCache Series, version 7.x does not allow NCM to establish sessions using SSH versions 1 and 2. It is recommended that you do not manage the Network Appliance Proxy via SSH and restrict device access to SNMP and Telnet only.

Netopia routers, OS version 4.8.x, 8.xx

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running)	X		
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces			
Modules and Inventory			
Flash Storage Space			
File System			
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: full username, full password, read-only community strings, read/ write community strings)	X		
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Known Issues

Errors during configuration deployment

The device configuration contains a comment, such as "; Netopia XXXX" and a masked password, such as "suppressor Name ******." If these commands are deployed to the device, the device will output a warning message. This message will appear in the task results and may flag the task as failed.

Workaround:

Edit & Deploy the configuration and remove the offending lines. Then, deploy the configuration change.

Nortel Alteon Application Switch (AAS), 2424 series, OS version 22.0.3, OS Version 23.2.1

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access			
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running)	X		
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime			
ICMP Test	X		
Topology Parsing			
Duplex Mismatch Parsing			
Other			
Software Center			

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Nortel Alteon Switched Firewall (ASF), 5100 series, OS version 2.2.3.9

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment	X		
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			

FEATURE	CLI	SNMP	TFTP/CLI
Software Center	X		
Password Management (can modify: full username, full password, read-only community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Known Issues

Configuration changes containing errors may be captured

Nortel Alteon devices buffer configuration changes until they are saved and applied. There may be cases where these buffered changes contain errors that will not manifest until the configuration is saved. NCM may therefore capture a configuration state that contains these errors. Later, when the changes are saved, the device will discard all erroneous changes and NCM will end up with a copy of the device configuration that is not consistent with what is actually running on the device.

Avoid deploying software images with “.img” extensions

If you deploy an image with the extension ".img" to a Nortel Alteon device, it will reload and reset its configuration and default settings. Passwords will also be reset by the device. You should perform this task manually via the console port since the device must be reconfigured by the user following reload (refer to the *WLAN Security Switch 1.0 User's Guide and Command Reference*, Chapter 2, "Reinstalling the Software"). The preferred extension for images to deploy is “.pkg”.

Nortel Alteon SSL Accelerator, 3050 series, OS version 4.2.1

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment	X		
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			

FEATURE	CLI	SNMP	TFTP/CLI
Software Center			
Password Management (can modify: full username, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Known Issues

Configuration changes containing errors may be captured

Nortel Alteon devices buffer configuration changes until they are saved and applied. There may be cases where these buffered changes contain errors that will not manifest until the configuration is saved. NCM may therefore capture a configuration state that contains these errors. Later, when the changes are saved, the device will discard all erroneous changes and NCM will end up with a copy of the device configuration that is not consistent with what is actually running on the device.

Nortel Alteon SSL Accelerator/VPN Gateway, 3050 and 3070 series, OS version 4.2.1, 6.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, Console)	X		
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to running)	X		
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime		X	
ICMP Test	X		
Topology Parsing			
Duplex Mismatch Parsing			
Other			
Software Center			

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Known Issue

Configuration deployment

On the Nortel Alteon SSL Accelerator/VPN Gateway, configuration deployment can be done to the running configuration on the device. As a result, the deployed configuration is merged with the running version. It does not replace it, however. Keep in mind that you can edit the configuration prior to deploying it to the device.

Nortel Alteon 180 Series and Alteon ACEdirector (AD) Series, WebOS version 10.0

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to running)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			

FEATURE	CLI	SNMP	TFTP/CLI
Software Center	X		
Password Management (can modify: full username, full password, read-only community strings, read/ write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Known Issues

Configuration changes containing errors may be captured

Nortel Alteon devices buffer configuration changes until they are saved and applied. There may be cases where these buffered changes contain errors that will not manifest until the configuration is saved. NCM may therefore capture a configuration state that contains these errors. Later, when the changes are saved, the device will discard all erroneous changes and NCM will end up with a copy of the device configuration that is not consistent with what is actually running on the device.

Full access users in password management always match NCM user for device

The full access username and password available to manage through the Password management feature are the username and password used by NCM to log into the device. This means that the username and password for the device in NCM will change which username and password is managed in Password Management. The reason for this is that the device can only change the password of the user logged in.

Common Alteon custom command script and diagnostic mode

The mode for custom command scripts and diagnostics for all Nortel Alteon drivers is shared across a family of devices that use a similar, but not identical, operating system. This means that though many custom command scripts and diagnostics defined for the “Nortel Alteon exec” mode will be applicable to all devices supporting this mode, some will not work across all such devices.

In almost all cases, the potential damage of running a script. containing a command not supported by a given device will simply be that the script fails with an error.

You can use the “for specific driver” selection when defining a command script or diagnostic if you want to tailor it to one member of the family of devices. As an example, consider a diagnostic that runs the "/info/local" command. This diagnostic will run successfully on a Nortel Alteon WSS or SSL, but will fail on a Nortel Alteon ASF (which does not support this command). In defining such a diagnostic, you would want to choose only the WSS and SSL drivers as supported.

Nortel BayStack switches, BPS 2000, BayStack 380, 460, 470 & 5500 series, BoSS version 3.0

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP	Other
Driver Discovery	X	X			
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X	
Configuration					
Configuration Snapshot (Startup configuration captured: no)			X		X
Device information parsing (supported)					
Enhanced Layer2 Basic IP information parsing (supported)					
Configuration Deployment (destination: to startup with reboot)			X	X	
Diagnostics					
Routing Table					
OSPF Neighbors					
Interfaces	X				
Modules and Inventory	X				
Flash Storage Space					
File System	X				
Uptime		X			
ICMP Test	X				
Topology Parsing	X				
Duplex Mismatch Parsing					
Other					

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP	Other
Software Center	X				
Password Management (can modify: limited username, limited password, full username, full password, read-only community strings, read/write community strings)	X				
Syslog Configuration and Change Detection					
Custom Scripts and Diagnostics	X				
ACL Management (ACL parsing only)					
Configlet Parsing					

Known Issues

Periodic Telnet failures if device remains dormant

Occasionally, if the device is not accessed regularly it will fail to respond to Telnet sessions. You can create a simple command script to “wake up” the device on a regular basis. For example, create a command script that sends an arbitrary command to the device. In the event of a snapshot failure, you can run this command script a few times to “wake up” the device or you can set up the script to run on a regular basis to limit occurrences of this device failure.

If you schedule the script to run on a recurring basis, it should be setup to run as often as you poll devices on your network.

The command script to create for this purpose should have the following information defined:

- Name: Wake Up BayStack
- Description: Script to wake up BayStack device(s)
- Mode: Baystack initialization

- Driver: {select either the BayStack 470 driver or “All applicable drivers”}
- Script: show banner

Device configuration is binary with supplementary text data

The device stores its configuration in a binary format that cannot be decoded. NCM captures this configuration and then captures the output of a number of device diagnostics to provide a textual representation of the device's current configuration. The device will produce a different binary configuration on every snapshot, even if no actual configuration information on the device has changed. As a result, NCM ignores changes in the binary configuration and uses the captured device diagnostic text to determine if any significant configuration change has occurred since the last snapshot that requires a new configuration to be saved.

Note: *It is possible that this diagnostic data will not completely represent all configuration options on the device. It is recommended that you setup a regular “checkpoint” snapshot of the device once a week to ensure that any extra configuration information is being collected.*

Configuration deployment can change passwords and ignore settings

A configuration deployment to a BayStack 470 resets the full-access login password to the hard-coded default password (“secure”). The NCM configuration deployment script takes this into account by changing the authentication information in the database to match the hard-coded default. However, if the BayStack 470 is configured for RADIUS authentication, the full-access login password is hidden and the BayStack 470 continues to use RADIUS authentication. In the case of RADIUS authentication, NCM changes the database authentication information and relies on password fallback to access the device if there is a RADIUS authentication challenge.

Note: *Nortel has indicated that when doing a configuration deployment to the BayStack 470, the IP address settings remain unchanged (i.e., the deployed configuration's settings are ignored). Although these are the only settings explicitly cited by Nortel to be ignored, it is possible the BayStack 470 could ignore other settings in your deployed configuration.*

Real-time change detection via Syslog is not supported

The device does not send Syslog messages that can reliably indicated configuration changes. Therefore, real-time configuration change detection via Syslog is not available.

Updating Device Software

During an Update Device Software task on a Baystack device, there are times when the task takes longer than usual. As a result, NCM goes on to perform other tasks. This causes the Baystack device to stop the software update process before it has completed. However, NCM reports that the Update Device Software task was successful, even though the Baystack device is still running the original software.

A “switch_sleep” variable has been added that enables the Update Device Software task additional time to complete before NCM performs anything on the device. This variable is set to 0 by default. You can modify the variable to a positive value, thereby giving the Update Device Software task an additional number of seconds to complete before another task is started.

Nortel BayStack switches: BPS 2000, BayStack 470 & 5500 Series, BoSS version 3.1

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: no)	X		X	
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destination: to running)			X	
Diagnostics				
Routing Table				
OSPF Neighbors				
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System				
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing				
Other				

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Software Center	X			
Password Management (can modify: limited username, limited password, full username, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Known Issues

Periodic Telnet failures if device remains dormant

Occasionally, if the device is not accessed regularly it will fail to respond to Telnet sessions. You can create a simple command script to "wake up" the device on a regular basis. For example, create a new command script that sends an arbitrary command to the device. In the event of a snapshot failure, you can run this command script a few times to "wake up" the device or you can setup the script to run on a regular basis to limit occurrences of this device failure. If you schedule the script to run on a recurring basis, it should be setup to run as often as you poll devices on your network.

The command script to create for this purpose should have the following information defined:

- Name: Wake Up BayStack
- Description: Script to wake up BayStack device(s)
- Mode: Baystack initialization
- Driver: {select either the BayStack 470 driver or "All applicable drivers"}
- Script: show banner

SSH Discovery

For some OS versions, SSH is disabled after a software update. As a result, SSH discovery fails.

Automatic reload after a software update

For some OS versions, the device will automatically reload after a software update or diagnostic is deployed. For these OS versions, NCM does not wait long enough before running the device discovery task. As a result, all software updates are successfully deployed, however the device discovery task fails.

Workaround:

If the device discovery task fails, wait at least five minutes after the software update has completed and then run a new device discovery task to re-discover the device.

Deploying a configuration using SSH

When deploying a configuration using SSH that includes the auto-negotiation-advertisements port 1-24 command, the SSH session is interrupted. As a result, the configuration deployment fails.

Workaround:

Use Telnet when deploying a configuration.

Software version 4.3

Nortel BayStack 5520 devices running software version 4.3 will at times reboot after driver discovery and snapshot operations.

Workaround:

Upgrade (or downgrade) your Nortel BayStack 5520 devices to a different software version (e.g., 5.06 or 4.2). Alternatively, you can deactivate the devices or remove them from NCM.

Nortel BayStack switches: 325, 350 and 450 series

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP	Other
Driver Discovery	X	X			
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X	
Configuration					
Configuration Snapshot (Startup configuration captured: no)			X		X
Device information parsing (supported)					
Enhanced Layer2 Basic IP information parsing (supported)					
Configuration Deployment (destination: to startup with reboot)			X		
Diagnostics					
Routing Table					
OSPF Neighbors					
Interfaces					
Modules and Inventory	X				
Flash Storage Space					
File System					
Uptime		X			
ICMP Test					
Topology Parsing	X				
Duplex Mismatch Parsing					
Other					
Software Center	X				

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP	Other
Password Management (can modify: limited username, limited password, full username, full password, read-only community strings, read/write community strings)	X				
Syslog Configuration and Change Detection					
Custom Scripts and Diagnostics					
ACL Management					
Configlet Parsing					

Known Issues

TFTP configuration capture could fail

When NCM requests a snapshot of the device configuration, the task may report “Cannot find the file specified.” This error is caused by the filename handling on the device. The complete configuration filename string sent by NCM will occasionally be dropped from the device's buffer. As a result, the device is unable to find the exact filename in the TFTP directory.

Workaround:

To minimize this issue, when you add a BayStack 350 or 450 device to NCM, try setting the Snapshot task “Retry Count” for the device group to which the device belongs to Once or Twice. You can access these settings via the Pending Tasks page (Tasks --> Pending Tasks). In the Pending Tasks table, find the Task Type:Snapshot for the device or its device group (Host/Group column). In the Actions column, click “Edit”. This link displays the Edit Task:Snapshot page.

Deployed configurations will always indicate a configuration change

Any deployed configuration, whether it actually changes the device configuration or not, is displayed as a change in NCM. This is due to unavoidable incidental changes to the binary configuration file on the device whenever a configuration is deployed.

Software update requires multiple steps

BayStack 350 and 450 software updates require multiple images to be uploaded (typically Boot and Agent images). The device will reboot automatically after each image upload. Cisco makes the following recommendations with regards to software updates on these devices:

1. The recommended best practice is not to use a single task to do fully automated software updates on these devices in a production environment. Rather, the recommended engineering practice is to upload each image independently and verify the correct functioning of the device before proceeding to the next upload task. In this usage, each image is contained in its own Image Set.
2. If a fully automated update is desired and deemed safe, the recommended best practice is to use a Multi-Task Project to include two individual image updates. This will ensure the images are uploaded in the proper order, which is important to ensure a successful update.
3. Uploading images as a single Image Set within a single Software Update task may work within some environments. However, it is not recommended as the image upload order is not guaranteed.

Real-time change detection via Syslog is not supported

The device does not send Syslog messages that can reliably indicated configuration changes. Therefore, real-time configuration change detection via Syslog is not available.

Nortel Centillion ATM Switch, 50/100 Series, OS version 3.x

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment	X	
Diagnostics		
Routing Table		
OSPF Neighbors		
Interfaces	X	
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		X
ICMP Test	X	
Topology Parsing		X
Duplex Mismatch Parsing		
Other		
Software Center		

FEATURE	CLI	SNMP
Password Management (can modify: read-only community strings, read/write community strings)	X	
Syslog Configuration and Change Detection		
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Nortel routers, BayRS (SNMP/TI)

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP	FTP/CLI	FTP/SNMP
Driver Discovery	X	X				
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X		X	
Configuration						
Configuration Snapshot (Startup configuration captured: yes)			X	X	X	X
Device information parsing (supported)						
Enhanced Layer2 Basic IP information parsing (supported)						
Configuration Deployment (destination: to startup with reboot)			X		X	
Diagnostics						
Routing Table	X	X				
OSPF Neighbors	X	X				
Interfaces	X	X				
Modules and Inventory	X	X				
Flash Storage Space	X	X				
File System	X					
Uptime		X				
ICMP Test	X					

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP	FTP/CLI	FTP/SNMP
Topology Parsing	X					
Duplex Mismatch Parsing						
Other						
Software Center	X				X	
Password Management (can modify: limited username, limited password, full username, full password, read-only community strings, read/write community strings)	X				X	
Syslog Configuration and Change Detection	X					
Custom Scripts and Diagnostics						
ACL Management						
Configlet Parsing						

Known Issues

Discovery through CLI of Nortel ASN devices may fail due to high NCM server load

Nortel ASN devices may not be discovered through CLI when the NCM system is under heavy load, such as when there is extensive logging by the NCM system and concurrent tasks are running inventory discovery tasks with “store session log” enabled. As a result, ASN devices may not respond to CLI command queries fast enough and the discovery task may fail for some or all of these types of devices.

It is recommended that you set up ASN devices for SNMP access by the NCM server, or if this is not feasible, manually assign the driver to the devices exhibiting this behavior.

Unsupported OS versions will result in discovery failure

Due to problems encountered with various OS versions on BayRS devices, discovery of the driver is limited by an explicit list of OS versions. NCM will only discover the BayRS driver for OS versions it supports.

Workaround:

You can add additional OS versions to support your system if necessary. Contact Cisco Tech Support for more information.

Low memory may result in failed CLI login attempts

BayRS routers will deny CLI login attempts if there is not enough memory available to support them. On devices that are low on memory, such failures can cause NCM device tasks to fail unexpectedly. If the device is low on memory, you may see error messages such as:

```
Retrieve configuration via CLI (Warning: Timeout in executing
script: Failed to get to technician interface mode.)
```

If messages like this occur frequently in NCM, you may need to reboot your router to clear up memory. Adding memory to the device will prevent the error from occurring frequently.

Circuit names should avoid containing braces or backslashes

Circuit names on BayRS routers can be defined to contain braces ("{", "}") and "escaped" characters (e.g. "\n", "\}"). However, NCM will not be able to parse such circuit names properly and may truncate or otherwise misread the name of the circuit. The following circuit names would be parsed correctly by NCM:

```
circuit-name {Remote circuit}
circuit-name {Remote circuit
with a second line}
```

The following circuit names would not be parsed correctly by NCM:

```
circuit-name {Remote { office } San Jose}
circuit-name {Remote office circuit :\} }
```

Some configured Syslog servers may not receive messages

You can configure BayRS devices to send Syslog messages to multiple hosts. However, by default the device sends messages to only five of the configured hosts. You can use the "maximum-hosts" (in bcc) command to configure the device to use more or fewer Syslog hosts (with an absolute maximum of ten).

You can use the show "syslog log-host" command (in bcc) to confirm the operational state of Syslog messaging to the NCM server. If the operational state is down, remove any unnecessary Syslog servers from the device's configuration or increase the maximum-hosts value to at least one greater than the number of currently configured Syslog hosts.

To enable Syslog logging to the NCM server that was previously listed as down, save the configuration you modified and reload the device. Alternately, you can delete the Syslog host entry for the NCM server from the configuration and then use the NCM "Configure Syslog" task to add it back to the device.

Nortel Contivity VPN switches, 100 & 400 series

FEATURE	CLI	SNMP
Driver Discovery	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table	X	
OSPF Neighbors		
Interfaces	X	
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		X
ICMP Test	X	
Topology Parsing	X	
Duplex Mismatch Parsing	X	
Other		
Software Center		
Password Management (can modify: limited password, full password)	X	
Syslog Configuration and Change Detection	X	

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics	X	
ACL Management	X	
Configlet Parsing		

Nortel Ethernet Routing Switch 2500 series, OS Version 4.0

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment			
Diagnostics			
Routing Table			
OSPF Neighbors			
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center			

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: limited username, limited password, full username, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Nortel Contivity VPN switches, 600, 1100, 2500, 2600, 4500 & 4600 series

FEATURE	CLI	SNMP	FTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X		X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System			
Uptime		X	
ICMP Test	X		
Topology Parsing			
Duplex Mismatch Parsing	X		
Other			
Software Center			

FEATURE	CLI	SNMP	FTP/CLI
Password Management (can modify: full username, full password)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Nortel Contivity VPN switches, 600, 1100, 2500, 2600, 4500 & 4600 series (binary configuration)

FEATURE	CLI	SNMP	FTP/CLI
Driver Discovery	X	X	
General Access	X		X
Configuration			
Configuration Snapshot (Startup configuration captured: no)			X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destinations: to running, to startup with reboot)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System			
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing	X		
Other			
Software Center	X		

FEATURE	CLI	SNMP	FTP/CLI
Password Management (can modify: full username, full password)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Nortel Ethernet Routing Switch 4500 series, OS Version 5.0

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, Console)	X		
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment			
Diagnostics			
Routing Table			
OSPF Neighbors			
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center			

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Nortel GbE Switch Module for IBM Blade Center, OS version 1.2.2.0

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces			
Modules and Inventory	X		
Flash Storage Space			
File System			
Uptime			
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Nortel OPTera Metro Ethernet Service Modules 1400/ 1450 version 1.2.x, 1.3.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)			X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment			
Diagnostics			
Routing Table			
OSPF Neighbors			
Interfaces	X		
Modules and Inventory		X	
Flash Storage Space			
File System			
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center			

FEATURE	CLI	SNMP	TFTP/CLI
Password Management			
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Known Issues

Enabling Telnet passwords

You might need to manually run the ‘cli password telnet local’ command if you do not currently use passwords for Telnet on the Nortel OME device. Keep in mind that although you are prompted for a username when configuring passwords, the Nortel OME device discards the username value.

Configuration deployment

If an identical configuration is deployed to the Nortel OPTera device, sections of the deployed configuration will be ignored. In addition, passwords will be changed to hard-coded defaults.

SNMP discovery

SNMP discovery on the Nortel OPTera device is more reliable than CLI discovery. As a result, it is recommended that you use SNMP discovery whenever possible.

Nortel Passport routers, 1200 series

FEATURE	CLI	SNMP	TFTP	TFTP/CLI	FTP/CLI
Driver Discovery	X	X			
General Access (CLI protocols: Telnet, Console)	X	X			X
Configuration					
Configuration Snapshot (Startup configuration captured: no)	X				
Device information parsing (supported)					
Enhanced Layer2 Basic IP information parsing (supported)					
Configuration Deployment (destination: to running)				X	
Diagnostics					
Routing Table	X				
OSPF Neighbors	X				
Interfaces	X				
Modules and Inventory	X				
Flash Storage Space					
File System					
Uptime					
ICMP Test	X				
Topology Parsing	X				
Duplex Mismatch Parsing					
Other					
Software Center					

FEATURE	CLI	SNMP	TFTP	TFTP/CLI	FTP/CLI
Password Management (can modify: full password, read-only community strings, read/write community strings)					
Syslog Configuration and Change Detection					
Custom Scripts and Diagnostics	X				
ACL Management					
Configlet Parsing					

Nortel Passport routers, 8000 series, and ERS routers, 1600 and 8000 series

FEATURE	CLI	SNMP	FTP/CLI	OTHER
Driver Discovery	X	X		
General Access (CLI protocols: SSH1, Telnet, Console)	X	X	X	
Configuration				
Configuration Snapshot (Startup configuration captured: no)	X			
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destination: to running)			X	
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing				
Other				

FEATURE	CLI	SNMP	FTP/CLI	OTHER
Software Center	X			X
Password Management (can modify: full username, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management	X			
Configlet Parsing				

Known Issues

Limited username and password management

NCM can manage one of the four lesser privileged access levels on the Passport 8600, with limitations. The access level managed by NCM is "ro". To initially manage the "ro" account, the Passport 8600 must have that privilege/account in the default state (where the username, password, and access level match). For example, the Passport 8600 must have the "ro" account enabled with the username and password set to "ro".

VLAN parsing

Nortel Passport routers support different types of VLANs depending on the protocol (byport, byipsubnet, byprotocol, bysrcmac, bysvlan, or forIDS) used. A port will only be mapped to a VLAN if it is assigned in only one VLAN regardless of the VLAN's protocol. In addition, the configuration does not display the protocol used for VLAN1 (the default VLAN) nor the ports assigned to it. As a result, VLAN1 will not contain any ports.

SSH v2 disabled for passport devices

SSH v1 has been enabled to work with Passport and Nortel Ethernet Routing Switch (ERS) devices. SSH v2, however, might encounter protocol errors with NCM and is not currently supported.

Passport OS versions prior to 3.2 reset password when deploying to startup

Performing a deploy configuration to startup and reboot task in NCM against a Passport 8000 series device running an OS version of 3.1.x or earlier will result in the passwords on the device being reset to a default value. NCM does not detect this change and will therefore lose access via CLI to the device in this event (some tasks may continue to work if SNMP access is still available).

Cisco recommends not managing Passport 8000 or 8300 series devices running OS versions prior to 3.2. If this must be done, it is important to not perform configuration deployments to startup via NCM.

Software update requires special handling in NCM

Updating software on a Passport 8000 series device involves several steps to ensure a successful update. Before deploying software to this device, please review the *Nortel Passport 8000 Series Devices Software Update Guide*. This guide describes how to enable updates for Passport 8000 devices in NCM and the steps necessary to ensure successful software deployments.

Nortel Passport routers, 1600 series

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)			X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running and to startup with reboot)			X
Diagnostics			
Routing Table	X	X	
OSPF Neighbors	X	X	
Interfaces			
Modules and Inventory			
Flash Storage Space			
File System			
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: full username, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Nortel Passport, 6400 series

FEATURE	CLI	FTP/CLI
Driver Discovery	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)		X
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table	X	
OSPF Neighbors		
Interfaces	X	
Modules and Inventory	X	
Flash Storage Space		
File System		
Uptime		
ICMP Test		
Topology Parsing	X	
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management (can modify: full username, full password)	X	
Syslog Configuration and Change Detection		

FEATURE	CLI	FTP/CLI
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Nortel Secure Router (Tasman) models 1001, 1002, 1004, 1400, 3120, 4100, and 6302

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: yes)	X		
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			

FEATURE	CLI	SNMP	TFTP/CLI
Software Center			
Password Management			
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics (bulk deploy available)	X		
ACL Management			
Configlet Parsing			

Known Issues

Nortel Secure Router (Tasman) 1001 and 3120

The Nortel Secure Router (Tasman) 1001 (running OS version 8.1) and Nortel Secure Router 3120 (running OS version 9.0) have been tested and verified to work with the Driver Discovery and Configuration Snapshot functionality. Advanced functionality, such as Custom Scripts and Diagnostics, might work, but to date have not been tested.

Nortel Secure Routers (Tasman) running OS version 8.4

The Nortel Secure Router (Tasman) traditionally used a string, terminated by the hash sign (#) character to delimit the default prompt for the administrative login terminating character. With OS version 8.4, the administrative login terminating character prompt is user-definable. As a result, the Nortel Secure Router (Tasman) driver supports three possible terminating characters, including the:

- Hash sign (#)
- Greater than symbol (>)
- Percent sign (%)

Assigning a terminating character other than one of characters listed above results in a failed CLI discovery and additional indeterminate results.

SSHv2 not supported for OS versions 7.0.5 and 7.1.1

SSHv2 was first implemented in OS version 7.2. There is no SSHv2 support in earlier OS versions 7.0.5 or 7.1.1.

Nortel VPN Routers 1750/2700/5000 series

FEATURE	CLI	SNMP	FTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)			X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory	X	X	
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center			
Password Management (can modify: full username, full password)	X		

FEATURE	CLI	SNMP	FTP/CLI
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Known Issues

Using TFTP for Configuration Deployment

When using TFTP for configuration deployment (Deploy to Running) on a Adtran NetVanta 3200 device, DNS server settings may not be configured properly due to the way the device handles the 'ip name-server <address>' command if the device perceives an existing DNS entry in the string. If a name server address being deployed is already configured on the device, any address(es) following that entry are ignored.

For example:

A current configuration has the entry 'ip name-server x.x.x.x y.y.y.y z.z.z.z'. If the entry 'ip name-server w.w.w.w z.z.z.z' is deployed, the w.w.w.w address is added to the configuration and an error is triggered because the z.z.z.z address is already listed in the configuration.

If the entry 'ip name-server z.z.z.z w.w.w.w' is deployed, the w.w.w.w address is ignored and will not be added to the configuration. However, if a new string, such as 'ip name-server t.t.t.t u.u.u.u' is deployed, both addresses will be configured.

Deploy Passwords Task

If the FTP server is not enabled on the Nortel VPN Router, models 1750/2700/5000, OS version 07_00.062, the Deploy Passwords task is marked as failed. However, the task is successfully run. This is due to the failure of the automatic snapshot triggered by the Deploy Passwords task.

Nortel VPN Router 1700/1740/1750 series

FEATURE	CLI	SNMP	FTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)			X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory	X	X	
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center			
Password Management (can modify: full username, full password)	X		

FEATURE	CLI	SNMP	FTP/CLI
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Known Issue

Deploy Passwords Task

If the FTP server is not enabled on the Nortel VPN Router, models 1700/1740/1750 series, OS version 07_00.062, the Deploy Passwords task is marked as failed. However, the task is successfully run. This is due to the failure of the automatic snapshot triggered by the Deploy Passwords task.

Nortel WAP, 2221 series, OS version 1.2.0

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: no)	X			
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment	X			
Diagnostics				
Routing Table				
OSPF Neighbors				
Interfaces	X			
Modules and Inventory				
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing				
Other				
Software Center	X			

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Password Management (can modify: full username, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management				
Configlet Parsing				

Known Issues

SNMP community strings not available from device

The Nortel WLAN access point does not provide its SNMP community strings in its configuration. As a result, NCM will not be able to determine automatically if SNMP community strings change. Any change to SNMP community strings on the device will require editing the device in NCM to update the SNMP community strings to use.

Model only available through SNMP access

The model information for Nortel WLAN access points is only available through SNMP access. If SNMP access is disabled or the community string NCM is specified to use is incorrect for the device, this information will not be retrieved.

Nortel WLAN Switch, WSS 2250 series, OS version 1.0.0

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running)	X		
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: full username, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Known Issues

Configuration changes containing errors may be captured

Nortel Alteon devices buffer configuration changes until they are saved and applied. There may be cases where these buffered changes contain errors that will not manifest until the configuration is saved. Consequently, NCM could capture a configuration that contains errors. Later, when the changes are saved, the device will discard all erroneous changes and NCM could have a copy of the device configuration that is not consistent with what is actually running on the device.

Changes to certificates and RSA keys will not be detected

The certificates and private RSA keys are always masked when comparing configuration captures since they change with every “dump” command. If they were not masked, every snapshot would result in a detected configuration change and stored configuration. However, due to this masking, legitimate changes to these certificates and keys will not be detected. If you change this information in the configuration, you should take a “checkpoint” snapshot to force the saving of the configuration into NCM and ensure the modified keys are saved.

Startup configuration

Startup configuration retrieval requires TFTP to be enabled.

Deploy Passwords Task

The Deploy Passwords Task will parse and deploy only SNMP community strings with read-only and read-write access.

Software Center

Nortel WSS 23xx devices store firmware images on two partitions:

- An active partition, marked with *(ex: *boot1)
- A backup partition (ex: boot0)

Software Center always updates the image and boots the current backup partition.

Avoid deploying software images with “.img” extensions

If you deploy an image with the extension ".img" to a Nortel Alteon device, it will reload and reset its configuration and default settings. Passwords will also be reset by the device. You should perform this task manually via the console port since the device must be reconfigured by the user following reload (refer to the *WLAN Security Switch 1.0 User's Guide and Command Reference*, Chapter 2, "Reinstalling the Software").

The preferred extension for images to deploy is “.peg”.

Full access users in password management always match NCM user for device

The full access username and password available to manage through the Password management feature are the username and password used by NCM to login to the device. This means that the username and password for the device in NCM will change which username and password is managed in Password Management. The reason for this is that the device can only change the password of the logged-in user.

Common Alteon custom command script and diagnostic mode

The mode for custom command scripts and diagnostics for all Nortel Alteon drivers is shared across a family of devices that use a similar, but not identical, operating system. This means that though many custom command scripts and diagnostics defined for the “Nortel Alteon exec” mode will be applicable to all devices supporting this mode, some will not work across all such devices. In almost all cases, the potential damage of running a script containing a command not supported by a given device will simply be that the script fails with an error.

You can use the “for specific driver” selection when defining a command script or diagnostic if you want to tailor it to one member of the family of devices. As an example, consider a diagnostic that runs the “/info/local” command. This diagnostic will run successfully on a Nortel Alteon WSS or SSL, but will fail on a Nortel Alteon ASF (which does not support this command). In defining such a diagnostic, you would want to choose only the WSS and SSL drivers as supported.

WLAN Switch, WSS 2350, 2360, 2361 series, OS version 5.0

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: yes)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running, to startup with reboot)	X		X
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify: limited username, limited password, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Known Issues

Startup configuration

Startup configuration retrieval requires TFTP to be enabled.

Deploy Passwords Task

The Deploy Passwords Task will parse and deploy only SNMP community strings with read-only and read-write access.

Software Center

Nortel WSS 23xx devices store firmware images on two partitions:

- An active partition, marked with *(ex: *boot1)
- A backup partition (ex: boot0)

Software Center always updates the image and boots the current backup partition.

Packeteer PacketShaper, OS version 6.x, 7.x, 8.x

FEATURE	CLI	SNMP	FTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)			X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to startup with reboot)			X
Diagnostics			
Routing Table			
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center			X

FEATURE	CLI	SNMP	FTP/CLI
Password Management (can modify: limited password, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Known Issue

Enable_password and username required for FTP access

Packeteer devices must have the enable_password set to work with FTP. This is the password NCM uses to login to the device. In addition, Packeteer devices do not require a specific username to perform a Telnet session from the device. However, the username is needed when using FTP. When adding Packeteer devices to NCM, you must include a username in the Password Information section if you plan to connect to the device via FTP. If you do not include a username, NCM will set the username to 'user'. This is not a valid entry when connecting to the device via FTP. Consequently, no successful snapshots will be taken from this device.

Username required for FTP access

Packeteer devices do not require a specific username to perform a Telnet session from the device. However, the username is needed when using FTP. When adding Packeteer devices to NCM, you must include a non-empty string in the Password Information section if you plan to connect to the device via FTP. Otherwise, no successful snapshots will be taken from this device.

Incomplete configuration deployment

Due to device restrictions, NCM will not deploy changes that are displayed in the snapshot under the “Non-sharable (local) settings:” area.

Paradyne IP DSLAM, 4229 Series, OS version 2.x

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment (destination: to running and to startup with reboot)		
Diagnostics		
Routing Table	X	
OSPF Neighbors		
Interfaces	X	
Modules and Inventory	X	
Flash Storage Space		
File System	X	
Uptime		X
ICMP Test	X	
Topology Parsing	X	
Duplex Mismatch Parsing		
Other		
Software Center	X	
Password Management (can modify limited username, limited password, full password)	X	

FEATURE	CLI	SNMP
Syslog Configuration and Change Detection	X	
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Powerware ConnectUPS Web/SNMP Card V4.18

FEATURE	CLI	SNMP
Driver Discovery		X
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table		
OSPF Neighbors		
Interfaces		
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		
ICMP Test		
Topology Parsing		
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management (super user)	X	
Syslog Configuration and Change Detection		

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics		
ACL Management		
Configlet Parsing		

Procket routers, OS version 2.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: yes)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running and to startup with reboot)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify limited username, limited password, full password, read-only community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Qualcomm Flarion RadioRouter RR2045, 2.11.x and higher

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: SSH2, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment (destination: to running)	X	
Diagnostics		
Routing Table	X	
OSPF Neighbors		
Interfaces	X	
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		X
ICMP Test	X	
Topology Parsing		
Duplex Mismatch Parsing		
Other		
Software Center		

FEATURE	CLI	SNMP
Password Management (can modify read-only community strings, read/write community strings)	X	
Syslog Configuration and Change Detection		
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Radware, Load Balancer AppDirector, OS version 1.03.04

FEATURE	CLI	SNMP	TFTP/CLI	HTTP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH2, Console)	X	X	X	
Configuration				
Configuration Snapshot (Startup configuration captured: no)	X		X	
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destination: to running)			X	
Diagnostics				
Routing Table	X			
OSPF Neighbors	X			
Interfaces	X			
Modules and Inventory	X			
Flash Storage Space				
File System	X			
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing				
Other				
Software Center				X

FEATURE	CLI	SNMP	TFTP/CLI	HTTP
Password Management (can modify full username/ password, read/write community strings)	X			
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management				
Configlet Parsing				

Known Issues

Creating read/write SNMP community strings

To create read/write SNMP community strings, you can overwrite default values using the Device Access settings:

- snmp_view - the name of the view (for read and write access). If not specified, the value “default_view” is used.
- snmp_read_group - the name of the read only group. If not specified, the value “default_ro” is used.
- snmp_write_group - the name of the read/write group. If not specified, the value “default_rw” is used.

SNMP community strings

For NCM to support an SNMP community string, the View name for the access groups to which a particular SNMP community string is assigned must be the same regardless of the SNMP security model (snmp v1 or snmp v2).

For example:

```
manage snmp access create group-ro SNMPv1 noAuthNoPriv -rvn ReadOnlyView
manage snmp access create group-ro SNMPv2c noAuthNoPriv -rvn ReadOnlyView
manage snmp access create group-rw SNMPv1 noAuthNoPriv -rvn ReadOnlyView -wvn ReadWriteView
manage snmp access create group-rw SNMPv2c noAuthNoPriv -rvn ReadOnlyView -wvn ReadWriteView
```

(where the groups are `group-ro` and `group-rw`)

Radware, Linkproof AS1, OS version 4.35.X

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center			
Password Management (can modify full password, read-only community strings)	X		

FEATURE	CLI	SNMP	TFTP/CLI
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Known Issues

Configuration deployment

To modify an existing line from a configuration deployment, you must use the “set” command, not the “create” command. If you use the “create” command, your changes will not be committed. Keep in mind that this only applies to commands that include the “create” keyword.

Encrypted configuration files

For Radware devices, the configuration file sent through TFTP can be encrypted. In this case, NCM will skip to CLI-only configuration retrieval. It is recommended that you modify the TFTP file-type to CLI, for example:

```
manage tftp file-type set 1
```

Note: The “file-type” parameter can accept only one of the following values: `cli` or `ber`.

Riverbed Steelhead 520, x010 series, OS version 3.x

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment (destination: to running)		
Diagnostics		
Routing Table	X	
OSPF Neighbors		
Interfaces	X	
Modules and Inventory	X	
Flash Storage Space		
File System		
Uptime		X
ICMP Test	X	
Topology Parsing	X	
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management (can modify full password, read-only community strings)	X	

FEATURE	CLI	SNMP
Syslog Configuration and Change Detection	X	
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Riverstone RS2000, Cabletron OEM SSR2000 20 port Switch Router, Software Ver. E9.0.7.7 (Enterasys)

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: yes)	X		X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to startup with reboot)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory	X		
Flash Storage Space			
File System	X		
Uptime			
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			

FEATURE	CLI	SNMP	TFTP/CLI
Software Center			
Password Management (can modify limited password, full password)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Known Issue

Pre-task snapshots

There could be issues with tasks that require a pre-task snapshot being unable to re-login to the device. It is recommended that you retry the tasks or contact Support for assistance.

Secure Computing Sidewinder firewalls, G2, OS version 6.x

FEATURE	CLI	SNMP	SCP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment			X
Diagnostics			
Routing Table	X		
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing	X		
Other			
Software Center			

FEATURE	CLI	SNMP	SCP/CLI
Password Management (can modify: full password, read-only community strings)	X		
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Sonus GSX, OS V06.03.02 R004

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, Console)	X	
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table	X	
OSPF Neighbors		
Interfaces	X	
Modules and Inventory	X	
Flash Storage Space		
File System		
Uptime		
ICMP Test		
Topology Parsing		
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management		
Syslog Configuration and Change Detection		

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Symbol ES3000 switch, Device Series, OS version 1.0.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)			X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running)			X
Diagnostics			
Routing Table			
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime			
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center	X		

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify limited password)	X		
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics	X		
ACL Management			
Configlet Parsing			

Symbol Spectrum Access Point, AP-302x, OS version 04.02

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery		X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to startup with reboot)			X
Diagnostics			
Routing Table			
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime		X	
ICMP Test			
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			

FEATURE	CLI	SNMP	TFTP/CLI
Software Center	X		
Password Management			
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics			
ACL Management			
Configlet Parsing			

Known Issues

Password Management

The Symbol Spectrum Access Point is very discerning about accepting passwords. If anything goes wrong on the initial password entry, the device closes the connection. Consequently, the standard CLI discovery script does not work. (It sends a ^U and backspace before the password and these are treated as part of the login attempt.) In addition, once the device closes the connection, it goes into lock-down for a second or so, refusing all further login attempts. As a result, to discover the device, you must insert its discovery script prior to those scripts used for BayStack discovery.

Symbol Spectrum24 Access Point, AP-4100 series, OS version 02.x, 03.x

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery		X	
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X		X
Configuration			
Configuration Snapshot (Startup configuration captured: no)	X		
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to startup with reboot)			X
Diagnostics			
Routing Table			
OSPF Neighbors			
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System			
Uptime			
ICMP Test			
Topology Parsing			
Duplex Mismatch Parsing			
Other			

FEATURE	CLI	SNMP	TFTP/CLI
Software Center			
Password Management			
Syslog Configuration and Change Detection			
Custom Scripts and Diagnostics			
ACL Management			
Configlet Parsing			

Known Issues

Configuration Deployment (not reported by device)

The Symbol AP-41xx Access Point does not report errors when deploying a configuration before a restart. Rather, the device ignores errors and restarts with the last saved configuration. It is important to review any detected changes in the configuration after a configuration deployment to ascertain if the desired changes took effect.

Configuration Deployment (changes config filename and TFTP server)

Because the Symbol AP-41xx Access point reboots on deployment, a configuration deployment attempt results in the TFTP server being set to the NCM server used for the deployment. In addition, the config filename is set to the filename used by the NCM server for the deployment.

Configuration Deployment (changes to passwords or community strings could result in loss of connectivity)

Because passwords and community strings cannot be captured from the Symbol AP-41xx Access Point configuration, NCM has no way of knowing if they have changed. If an Edit & Deploy action is taken that includes changes to these values, NCM is not able to identify these changes and could lose connectivity to the device after the deployment. If this occurs, you will need to manually reconfigure NCM with the new passwords and/or community strings to restore connectivity with the device.

Symbol WS2000 802.11 a/b/g Wireless Switch, OS version 1.5.0.0-216r

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: no)	X		X	X
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment (destination: to running, startup with reboot)			X	
Diagnostics				
Routing Table	X			
OSPF Neighbors				
Interfaces	X			
Modules and Inventory				
Flash Storage Space				
File System				
Uptime				
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing				
Other				

FEATURE	CLI	SNMP	TFTP/CLI	TFTP/SNMP
Software Center				
Password Management (can modify full username, full password, read-only community strings, read/write community strings)	X			
Syslog Configuration and Change Detection				
Custom Scripts and Diagnostics	X			
ACL Management				
Configlet Parsing				

Known Issues

Software updates not supported

Software updates on the Symbol WS2000 requires the device to reboot into a Diagnostic mode. This method is not currently supported.

Syslog Configuration and Change Detection

The Symbol WS2000 does not send Syslog messages for Admin login/logoff or configuration changes.

Terayon routers, TeraComm System & TeraLink Gateway Series

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment (destination: to running)	X	
Diagnostics		
Routing Table	X	
OSPF Neighbors		
Interfaces	X	
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		X
ICMP Test	X	
Topology Parsing	X	
Duplex Mismatch Parsing		
Other		
Software Center		

FEATURE	CLI	SNMP
Password Management (can modify: limited username, limited password, full username, full password)	X	
Syslog Configuration and Change Detection		
Custom Scripts and Diagnostics	X	
ACL Management (ACL parsing only)		
Configlet Parsing		

Transition Networks CPSMM100-120, OS version 060117PQ

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table		
OSPF Neighbors		
Interfaces	X	
Modules and Inventory	X	
Flash Storage Space		
File System		
Uptime		X
ICMP Test	X	
Topology Parsing	X	
Duplex Mismatch Parsing		
Other		
Software Center		

FEATURE	CLI	SNMP
Password Management (can modify: limited password, full password)	X	
Syslog Configuration and Change Detection		
Custom Scripts and Diagnostics	X	
ACL Management (ACL parsing only)		
Configlet Parsing		

Tripp Lite PowerAlert, OS version 12.04.0019

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table		
OSPF Neighbors		
Interfaces		
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		X
ICMP Test		
Topology Parsing		
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management (can modify: full password)	X	
Syslog Configuration and Change Detection		

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics	X	
ACL Management (ACL parsing only)		
Configlet Parsing		

Unix servers, generic

FEATURE	CLI	SNMP
Driver Discovery	X	X
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X
Configuration		
Configuration Snapshot (Startup configuration captured: no)	X	
Device information parsing (supported)		
Enhanced Layer2 Basic IP information parsing (supported)		
Configuration Deployment		
Diagnostics		
Routing Table	X	
OSPF Neighbors		
Interfaces	X	
Modules and Inventory		
Flash Storage Space		
File System		
Uptime		X
ICMP Test	X	
Topology Parsing	X	
Duplex Mismatch Parsing		
Other		
Software Center		
Password Management		
Syslog Configuration and Change Detection		

FEATURE	CLI	SNMP
Custom Scripts and Diagnostics	X	
ACL Management		
Configlet Parsing		

Yamaha Router RTX1100

FEATURE	CLI	SNMP	TFTP/CLI
Driver Discovery	X	X	
General Access (CLI protocols: Telnet, SSH2, Console)	X	X	X
Configuration			
Configuration Snapshot (Startup configuration captured: yes)			X
Device information parsing (supported)			
Enhanced Layer2 Basic IP information parsing (supported)			
Configuration Deployment (destination: to running, startup with reboot)			X
Diagnostics			
Routing Table	X		
OSPF Neighbors	X		
Interfaces	X		
Modules and Inventory			
Flash Storage Space			
File System	X		
Uptime		X	
ICMP Test	X		
Topology Parsing	X		
Duplex Mismatch Parsing			
Other			
Software Center			X

FEATURE	CLI	SNMP	TFTP/CLI
Password Management (can modify limited username, limited password, full password, read-only community strings, read/write community strings)	X		
Syslog Configuration and Change Detection	X		
Custom Scripts and Diagnostics	X		
ACL Management	X		
Configlet Parsing			

Known Issue

File Verification Timeout

The Yamaha Router RTX1100's TFTP server includes a file verification feature that verifies the integrity of uploaded software before it sends the last TFTP ACK (acknowledgement) to the client. This verification process can take up to 20 seconds. As a result, it could take approximately 20 seconds for the client to receive the last ACK. By that time, NCM's TFTP client aborts the process and reports a software update error.

Workaround:

There is no workaround. Although the Software Update task reports a failure (due to the delayed ACK), the software upload completes successfully and the device is upgraded.

ZyXEL wireless devices, ZyWall & G-2000PLUS, OS version 3.62

FEATURE	CLI	SNMP	FTP	FTP/CLI
Driver Discovery	X	X		
General Access (CLI protocols: Telnet, SSH1, SSH2, Console)	X	X	X	X
Configuration				
Configuration Snapshot (Startup configuration captured: no)	X			
Device information parsing (supported)				
Enhanced Layer2 Basic IP information parsing (supported)				
Configuration Deployment				
Diagnostics				
Routing Table	X			
OSPF Neighbors				
Interfaces	X			
Modules and Inventory				
Flash Storage Space				
File System				
Uptime		X		
ICMP Test	X			
Topology Parsing	X			
Duplex Mismatch Parsing				
Other				
Software Center			X	

FEATURE	CLI	SNMP	FTP	FTP/CLI
Password Management				
Syslog Configuration and Change Detection	X			
Custom Scripts and Diagnostics	X			
ACL Management				
Configlet Parsing				

Index