145 Rio Robles
San Jose, CA 95134
+1 408-579-2800

Firmware Support

Extreme Networks Extreme Control Center (formerly NetSight)®

Version 7.0
March, 2016

This document provides firmware support information for the following Extreme Control Center applications:

Extreme Control Center Product Support

Extreme Control Center is designed to support the following Extreme Networks hardware product families. Refer to the Firmware Release Notes for the list of MIBs supported for the following product families.

7100-Series	G-Series	Summit Series
800-Series	I-Series	E4G Series
A-Series	K-Series	
B-Series	S-Series	
C-Series	ExtremeWireless	
D-Series	BlackDiamond Series	

Extreme Control Center supports up to 2500 devices. SNMP must be configured on your devices to allow them to be managed by Extreme Control Center.

NAC Manager Firmware Support

NAC Manager supports the following Extreme Networks and 3rd-party hardware products and firmware versions:

Product	Firmware Version
7100-Series	8.22.xx 8.31.xx 8.32.xx 8.42.xx
800-Series	1.02.01.xx
A4	6.61.xx 6.71.xx 6.81.xx
B5/C5	6.61.xx 6.71.xx 6.81.xx
D-Series	6.03.xx
E4G Series	15.4.1.3-patch1-2 or higher
ExtremeWireless Controller	9.12.xx 9.15.xx 9.21.xx 10.01.xx
I3	6.42.xx 6.61.xx
K-Series	8.02.xx 8.31.xx 8.32.xx 8.42.xx
S-Series	8.02.xx 8.31.xx 8.32.xx 8.42.xx
BlackDiamond Series	15.4.1.3-patch1-2 or higher
Summit Series	15.4.1.3-patch1-2 or higher
HP ProCurve Switch 5304XL	E.05.04
HP ProCurve Switch 2824	I.08.98
Cisco Catalyst 4500R	12.1(12c)EW
Cisco 3750	12.2(35)SE2 12.2(25)SEE2
Cisco 2950	12.1(22)EA5
Cisco Wireless(1)	7.2.110.0

[1]For a complete list of Cisco Wireless devices, refer to the Cisco Release Notes for Firmware Version 7.2.110.0.

Identity and Access VPN Integration Requirements

This section lists the VPN concentrators that are supported for use in Identity and Access VPN Deployment scenarios.

Supported Functionality: Authentication and Authorization (policy enforcement)
Cisco ASA
Enterasys XSR

Supported Functionality: Authentication
Juniper SA (requires an S-Series Stand Alone (SSA) system in order to provide access control)

NOTE: For all Identity and Access VPN Deployment scenarios, an S-Series Stand Alone (SSA) system is required to change authorization levels beyond the initial authorization, for example, when using assessment.

Policy Manager Firmware Support

Section 1 lists the hardware products and firmware versions supported by Policy Manager.
Section 2 lists the Policy Manager feature sets for the supported products.
Section 3 lists the Access Control and CoS Classification Rule Support for the supported products.

Section 1: Product/Firmware Versions Supported

Policy Manager supports the following Extreme Networks hardware products and firmware versions:

Product	Firmware Version
7100-Series	8.22.xx 8.31.xx 8.32.xx 8.42.xx
A4	6.61.xx 6.71.xx 6.81.xx
B5/C5	6.61.xx 6.71.xx 6.81.xx
D-Series	6.03.xx
Summit 440G2/620	21.1.1.xx
Summit 450G2/460G2/670G2/770G2	16.1.1.xx 21.1.1.xx
ExtremeWireless Controller	9.12.xx 9.15.xx 9.21.xx 10.01.xx
I3	6.42.xx 6.61.xx
K-Series	8.02.xx 8.31.xx 8.32.xx 8.42.xx
S-Series	8.02.xx 8.31.xx 8.32.xx 8.42.xx

Section 2: Policy Manager Feature Support

- 7100-Series
- A4
- B5/C5
- D2
- Summit 440G2/620
- Summit 450G2/460G2/670G2/770G2
- I3
- K-Series/S-Series
- ExtremeWireless Controller

Feature Support 7100-Series

Functionality	7100-Series **8.22.xx** **8.31.xx** **8.32.xx** **8.42.xx**
Authentication Support	X
802.1X	X
MAC	X
MAC Mask	X
Web-Based	X
CEP	X
Quarantine	X(1)
Auto Tracking	X(1)
Global Authentication Settings:	X
Authentication Timeout	X
Current # of Authenticated Users	X
Multi-Users per Port	X
RFC3580 VLAN Authorization	X
RFC3580 VLAN Egress	X
RADIUS Support	X
RADIUS Accounting	X
RADIUS Response Mode	X
Priority Support (802.1p)	X
Policy Support	X
Policy-based VLAN Egress	X
Tagged Packet VLAN to Role Mapping	-
Authentication-based VLAN to Role Mapping	X
IP to Role Mapping	-
MAC to Role Mapping	X(2)
Rule Accounting	-
Port Disabled on Rule Hit	-
Disable Traffic Classify Type	-
Clear Rule Usage	-
Invalid Policy Action	X
Passive Domain Mode	-
Role-Based Actions:	-
TCI Overwrite	X(3)
SysLog/AuditTrap/DisablePort	-
Role-Based Traffic Mirror	-
Rule-Hit Actions:	-
SysLog/AuditTrap/DisablePort Prohibit	-
Rule-Based Traffic Mirror	-
Rule-Based TCI Overwrite	-
Egress Policy	-
Rate Limiting	X
MAC Locking	X
ToS/DSCP Rewrite	X
Anti-Spoofing	-

[1]Supported on 8.20.xx and higher.
[2]Only Port-level Source MAC to Role Mappings supported.
[3]TCI Overwrite functionality for a role is enabled by default on the 7100-Series device and cannot be changed via Policy Manager. Policy Manager ignores this setting.

Feature Support A4

Functionality	A4 Firmware Version 6.61.xx 6.71.xx 6.81.xx
Authentication Support	X
802.1X	X
MAC	X
MAC Mask	X
Web-Based	X
CEP	X(1)
Quarantine	-
Auto Tracking	-
Global Authentication Settings:	X
Authentication Timeout	X
Current # of Authenticated Users	X
Multi-Users per Port	X(2)
RFC3580 VLAN Authorization	X
RFC3580 VLAN Egress	X
RADIUS Support	X
RADIUS Accounting	X(3)
RADIUS Response Mode	X
Priority Support (802.1p)	X
Policy Support	X(4)
Policy-based VLAN Egress	X
Tagged Packet VLAN to Role Mapping	X(5)
Authentication-based VLAN to Role Mapping	X
IP to Role Mapping	-
MAC to Role Mapping	-
Rule Accounting	-
Port Disabled on Rule Hit	-
Disable Traffic Classify Type	-
Clear Rule Usage	-
Invalid Policy Action	-
Passive Domain Mode	-
Role-Based Actions:	-
SysLog/AuditTrap/DisablePort	-
Role-Based Traffic Mirror	-
Rule-Hit Actions:	-
SysLog/AuditTrap/DisablePort Prohibit	-
Rule-Based Traffic Mirror	-
Rule-Based TCI Overwrite	-
Egress Policy	-
Rate Limiting	X(6)
MAC Locking	X
ToS/DSCP Rewrite	X
Anti-Spoofing	-

[1]Supported on 6.71.xx and higher.
[2]One authenticated user and one VoIP phone (with VLAN tagged VoIP traffic) per port.
[3]Supported on 6.81.xx and higher.
[4]See Firmware Release Notes for details.
[5]This feature will not work properly unless the "Number of Users Allowed" attribute on a port is set to 2 or more. Only one device-level VLAN to Role mapping is supported.
[6]Priority-Based rate limits inbound only. GE ports - 8 rate limits (Priority 0 only); FE ports - 2 rate limits (Priorities 0,1,2,3 and 4,5,6,7). Role-Based rate limits supported.

Feature Support B5/C5

Functionality	B5/C5 Firmware Version 6.61.xx 6.71.xx 6.81.xx
Authentication Support	X
802.1X	X(1)
MAC	X(1)
MAC Mask	X
Web-Based	X(1)
CEP	X(2)
Quarantine	-
Auto Tracking	-
Global Authentication Settings:	X
Authentication Timeout	X
Current # of Authenticated Users	X
Multi-Users per Port	X(3)
RFC3580 VLAN Authorization	X
RFC3580 VLAN Egress	X
RADIUS Support	X
RADIUS Accounting	X(4)
RADIUS Response Mode	X
Priority Support (802.1p)	X
Policy Support	X
Policy-based VLAN Egress	X
Tagged Packet VLAN to Role Mapping	X(5)
Authentication-based VLAN to Role Mapping	X
IP to Role Mapping	-
MAC to Role Mapping	-
Rule Accounting	-
Port Disabled on Rule Hit	-
Disable Traffic Classify Type	-
Clear Rule Usage	-
Invalid Policy Action	-
Passive Domain Mode	-
Role-Based Actions:	-
SysLog/AuditTrap/DisablePort	-
Role-Based Traffic Mirror	-
Rule-Hit Actions:	-
SysLog/AuditTrap/DisablePort Prohibit	-
Rule-Based Traffic Mirror	-
Rule-Based TCI Overwrite	-
Egress Policy	-
Rate Limiting	X(6)
MAC Locking	X
ToS/DSCP Rewrite	X
Anti-Spoofing	-

[1]Can be enabled at the device-level and port-level with a maximum of four concurrent active sessions. However, there can be only one active Web-Based (PWA) session at a time.
[2]Supported on 6.71.xx only. CEP detection is not supported.
[3]B5 supports four users per port. C5 supports eight users per port. See Firmware Release Notes.
[4]Supported on 6.81.xx and higher.
[5]This feature will not work properly unless the "Number of Users Allowed" attribute on a port is set to 2 or more. Supported on both device and port level, but only one mapping is allowed at the device level and on each port.
[6]For Role-Based Rate Limiting, any rate limit specified by a Class of Service in a rule will be ignored. Only the role's Default Class of Service is used to specify the rate limit and this rate limit is applied to all traffic using this role.

Feature Support D2

Functionality	D2 Firmware Version 1.00.xx 6.03.xx
Authentication Support	X
802.1X	X(1)
MAC	X(1)
MAC Mask	X
Web-Based	X(1)
CEP	-
Quarantine	-
Auto Tracking	-
Global Authentication Settings:	X
Authentication Timeout	X
Current # of Authenticated Users	X
Multi-Users per Port	X(2,3)
RFC3580 VLAN Authorization	X
RFC3580 VLAN Egress	X
RADIUS Support	X
RADIUS Accounting	-
RADIUS Response Mode	X(4)
Priority Support (802.1p)	X
Policy Support	X(1)
Policy-based VLAN Egress	X
Tagged Packet VLAN to Role Mapping	X(5)
Authentication-based VLAN to Role Mapping	X
IP to Role Mapping	-
MAC to Role Mapping	-
Rule Accounting	-
Port Disabled on Rule Hit	-
Disable Traffic Classify Type	-
Clear Rule Usage	-
Invalid Policy Action	-
Passive Domain Mode	-
Role-Based Actions:	-
SysLog/AuditTrap/DisablePort	-
Role-Based Traffic Mirror	-
Rule-Hit Actions:	-
SysLog/AuditTrap/DisablePort Prohibit	-
Rule-Based Traffic Mirror	-
Rule-Based TCI Overwrite	-
Egress Policy	-
Rate Limiting	X(6)
MAC Locking	X(3)
ToS/DSCP Rewrite	X(7)
Anti-Spoofing	-

[1]Can be enabled at the device-level and port-level, but there can be only one active session at a time.
[2]Supports one authenticated user and one VoIP phone (with VLAN tagged VoIP traffic) per port.
[3]Dynamic MAC locking supported. Static MAC Locking supported only if Policy support is enabled.
[4]The Filter ID with VLAN Tunnel Attribute mode (Hybrid Mode) is not supported on D2 devices.
[5]This feature will not work properly, unless the "Number of Users Allowed" attribute on a port is set to 2 or more. Only one device-level VLAN to Role mapping is supported.
[6]Priority-Based rate limits inbound only. GE ports - 8 rate limits (Priority 0 only); FE ports - 2 rate limits (Priorities 0,1,2,3 and 4,5,6,7). Role-Based rate limits supported.
[7]Only if Policy Support is enabled.

Feature Support Summit 440G2/620

	Summit 440G2/620 Firmware Version
Functionality	**21.1.1.xx**
Authentication Support	X
802.1X	X
MAC	X
MAC Mask	X
Web-Based	-
CEP	-
Quarantine	-
Auto Tracking	-
Global Authentication Settings:	X
Authentication Timeout	X
Current # of Authenticated Users	X
Multi-Users per Port	X(1)
RFC3580 VLAN Authorization	X
RFC3580 VLAN Egress	X
RADIUS Support	X
RADIUS Accounting	X
RADIUS Response Mode	X
Priority Support (802.1p)	X
Policy Support	X
Policy-based VLAN Egress	X
Tagged Packet VLAN to Role Mapping	-
Authentication-based VLAN to Role Mapping	X
IP to Role Mapping	-
MAC to Role Mapping	X(2)
Rule Accounting	-
Port Disabled on Rule Hit	-
Disable Traffic Classify Type	-
Clear Rule Usage	-
Invalid Policy Action	X
Passive Domain Mode	-
Role-Based Actions:	-
TCI Overwrite	X(3)
SysLog/AuditTrap/DisablePort	-
Role-Based Traffic Mirror	-
Rule-Hit Actions:	-
SysLog/AuditTrap/DisablePort Prohibit	-
Rule-Based Traffic Mirror	-
Rule-Based TCI Overwrite	-
Egress Policy	-
Rate Limiting	X
MAC Locking	X
ToS/DSCP Rewrite	X
Anti-Spoofing	-

[1]Supports Active/Default and Active/Discard Only.
[2]Only Port-level MAC (Source)-to-Role Mappings supported.
[3]TCI Overwrite functionality can only be enabled for the Role.

Feature Support Summit 450G2/460G2/670G2/770G2

	Summit 450G2/460G2/670G2/770G2 Firmware Version
Functionality	**16.1.1.xx 21.1.1.xx**
Authentication Support	X
802.1X	X
MAC	X
MAC Mask	X
Web-Based	-
CEP	-
Quarantine	-
Auto Tracking	-
Global Authentication Settings:	X
Authentication Timeout	X
Current # of Authenticated Users	X
Multi-Users per Port	X(1)
RFC3580 VLAN Authorization	X
RFC3580 VLAN Egress	X
RADIUS Support	X
RADIUS Accounting	X
RADIUS Response Mode	X
Priority Support (802.1p)	X
Policy Support	X
Policy-based VLAN Egress	X
Tagged Packet VLAN to Role Mapping	-
Authentication-based VLAN to Role Mapping	X -
IP to Role Mapping	X(2)
MAC to Role Mapping	-
Rule Accounting	-
Port Disabled on Rule Hit	-
Disable Traffic Classify Type	-
Clear Rule Usage	X
Invalid Policy Action	-
Passive Domain Mode	-
Role-Based Actions:	X(3)
TCI Overwrite	-
SysLog/AuditTrap/DisablePort	-
Role-Based Traffic Mirror	-
Rule-Hit Actions:	-
SysLog/AuditTrap/DisablePort Prohibit	-
Rule-Based Traffic Mirror	-
Rule-Based TCI Overwrite	-
Egress Policy	
Rate Limiting	X
MAC Locking	X
ToS/DSCP Rewrite	X
Anti-Spoofing	-

[1]Supports Active/Default and Active/Discard Only.
[2]Only Port-level MAC (Source)-to-Role Mappings supported.
[3]TCI Overwrite functionality can only be enabled for the Role.

Feature Support I3

Functionality	I3 Firmware Version 6.42.xx 6.61.xx
Authentication Support	X
802.1X	X(1)
MAC	X(1)
MAC Mask	X
Web-Based	X(1)
CEP	-
Quarantine	-
Auto Tracking	-
Global Authentication Settings:	-
Authentication Timeout	-
Current # of Authenticated Users	-
Multi-Users per Port	-
RFC3580 VLAN Authorization	X
RFC3580 VLAN Egress	X
RADIUS Support	X
RADIUS Accounting	-
RADIUS Response Mode	-
Priority Support (802.1p)	X
Policy Support	X(2)
Policy-based VLAN Egress	X
Tagged Packet VLAN to Role Mapping	-
Authentication-based VLAN to Role Mapping	-
IP to Role Mapping	-
MAC to Role Mapping	-
Rule Accounting	-
Port Disabled on Rule Hit	-
Disable Traffic Classify Type	-
Clear Rule Usage	-
Invalid Policy Action	-
Passive Domain Mode	-
Role-Based Actions:	-
SysLog/AuditTrap/DisablePort	-
Role-Based Traffic Mirror	-
Rule-Hit Actions:	-
SysLog/AuditTrap/DisablePort Prohibit	-
Rule-Based Traffic Mirror	-
Rule-Based TCI Overwrite	-
Egress Policy	-
Rate Limiting	X
MAC Locking	X
ToS/DSCP Rewrite	X
Anti-Spoofing	-

[1]Can be enabled at the device-level and port-level, but there can only be one active session at a time.
[2]See Firmware Release Notes for details.

Feature Support K-Series/S-Series

Functionality	K-Series/S-Series Firmware Version 8.21.xx 8.31.xx 8.32.xx 8.42.xx
Authentication Support	X(1)
802.1X	X
MAC	X
MAC Mask	X
Web-Based	X
CEP	X
Quarantine	X(2)
Auto Tracking	X(2)
Global Authentication Settings:	X
Authentication Timeout	X
Current # of Authenticated Users	X
Multi-Users per Port	X
RFC3580 VLAN Authorization	X
RFC3580 VLAN Egress	X
RADIUS Support	X
RADIUS Accounting	X
RADIUS Response Mode	X
Priority Support (802.1p)	X
Policy Support	X
Policy-based VLAN Egress	X
Tagged Packet VLAN to Role Mapping	X
Authentication-based VLAN to Role Mapping	X
IP to Role Mapping	X
MAC to Role Mapping	X
Rule Accounting	X
Port Disabled on Rule Hit	X
Disable Traffic Classify Type	X
Clear Rule Usage	X
Invalid Policy Action	X
Passive Domain Mode	X
Role-Based Actions:	X
SysLog/AuditTrap/DisablePort	X
Role-Based Traffic Mirror	X
Rule-Hit Actions:	X
SysLog/AuditTrap/DisablePort Prohibit	X
Rule-Based Traffic Mirror	X
Rule-Based TCI Overwrite	X
Egress Policy	X(3)
Rate Limiting	X(4)
MAC Locking	X
ToS/DSCP Rewrite	X
Anti-Spoofing	X(2)

[1]The maximum number of users per device can be increased if an appropriate key is entered using the CLI on the device. Refer to the firmware documentation for more details.
[2]Supported on 8.02.xx and later only.
[3]Supported on 7.31.xx and later only.
[4]Priority-Based rate limits not supported.

Feature Support ExtremeWireless Controller

Functionality	ExtremeWireless Controller 9.12.xx 9.15.xx 9.21.xx 10.01.xx
Authentication Support	-
802.1X	-
MAC	-
MAC Mask	-
Web-Based	-
CEP	-
Quarantine	-
Auto Tracking	-
Global Authentication Settings:	-
Authentication Timeout	-
Current # of Authenticated Users	-
Multi-Users per Port	-
RFC3580 VLAN Authorization	-
RFC3580 VLAN Egress	-
RADIUS Support	X(1)
RADIUS Accounting	X(2)
RADIUS Response Mode	-
Priority Support (802.1p)	-
Policy Support	X
Policy-based VLAN Egress	X(3)
Tagged Packet VLAN to Role Mapping	-
Authentication-based VLAN to Role Mapping	-
IP to Role Mapping	-
MAC to Role Mapping	-
Rule Accounting	-
Port Disabled on Rule Hit	-
Disable Traffic Classify Type	-
Clear Rule Usage	-
Invalid Policy Action	-
Passive Domain Mode	-
Role-Based Actions:	-
SysLog/AuditTrap/DisablePort	-
Role-Based Traffic Mirror	-
Rule-Hit Actions:	-
SysLog/AuditTrap/DisablePort Prohibit	-
Rule-Based Traffic Mirror	-
Rule-Based TCI Overwrite	-
Egress Policy	-
Rate Limiting	X(4)
MAC Locking	-
ToS/DSCP Rewrite	-
Anti-Spoofing	-

[1]The RADIUS Authentication Client Status will display the current read-only setting. The status is automatically set to Enabled by the device when one or more RADIUS authentication servers are added.
[2]RADIUS accounting set up is configurable via Policy Manager. However, the ability to enable RADIUS accounting on an SSID is not configurable via Policy Manager.
[3] Supported on 8.31.xx and later only.
[4]Only the role's Default Action Class of Service is used to specify rate limits for the ExtremeWireless Controller. Role-Based rate limit is per user.

Section 3: Access Control/CoS Classification Rule Support

- 7100-Series
- A4
- B2/C2/D2 and B3/C3/G3/B5/C5
- Summit 440G2/620
- Summit 450G2/460G2/670G2/770G2
- I3
- K-Series and S-Series
- ExtremeWireless Controller
- A2

Rule Support 7100-Series

		7100-Series	
		Access Control	**CoS**
Layer 2	Ethertype	Permit/Deny (Ethertype w/ masking)	YES (Ethertype w/ masking)
	DSAP/SSAP	NO	NO
	MAC Address Source/ Destination/Bilateral	Permit/Deny (MAC w/ masking)	YES (MAC w/ masking)
	VLAN ID	NO	NO
	Priority	NO	NO
Layer 3	IP Type of Service	Permit/Deny (TOS w/ masking)	YES (TOS w/ masking)
	IP Protocol Type	Permit/Deny (Protocol w/ masking)	YES (Protocol w/ masking)
	IP Address Source/ Destination/Bilateral	Permit/Deny (IP w/ masking)	YES (IP w/ masking)
	IP Socket Source/ Destination/Bilateral	Permit/Deny (port w/ masking)	YES (port w/ masking)
	IP Fragment	Permit/Deny	YES
	IPX Class of Service	NO	NO
	IPX Packet Type	NO	NO
	IPX Network Source/ Destination/Bilateral	NO	NO
	IPX Socket Source/ Destination/Bilateral	NO	NO
	ICMP	NO	NO
	IPv6 Address Destination	Permit/Deny (IP w/ masking)	YES (IP w/ masking)
	IPv6 Socket Source/ Destination/Bilateral	NO	NO
	IPv6 Flow Label	NO	NO
	ICMPv6	NO	NO
	IP Time to Live (TTL)	Permit/Deny	YES
Layer 4	IP UDP Port Source/ Destination/Bilateral	Permit/Deny (IP w/ masking)	YES (IP w/ masking)
	IP TCP Port Source/ Destination/Bilateral	Permit/Deny (IP w/ masking)	YES (IP w/ masking)
	IP UDP Port Source/ Destination/Bilateral Range	Permit/Deny (IP w/ masking)	YES (IP w/ masking)
	IP TCP Port Source/ Destination/Bilateral Range	Permit/Deny (IP w/ masking)	YES (IP w/ masking)
Layer 7	Application	NO	NO

Rule Support A4

		A4	
		Access Control	**CoS**
Layer 2	Ethertype	Permit/Deny/VLAN (range)	YES (range)
	DSAP/SSAP	NO	NO
	MAC Address Source/ Destination/Bilateral	Permit/Deny Only (MAC masking)	YES (MAC masking)
	VLAN ID	NO	NO
	Priority	NO	NO
Layer 3	IP Type of Service	Permit/Deny Only	YES
	IP Protocol Type	Permit/Deny Only (range)	YES (range)
	IP Address Source/ Destination/Bilateral	Permit/Deny Only (IP masking)	YES (IP masking)
	IP Socket Source/ Destination/Bilateral	Permit/Deny Only (port w/ masking)	YES (port w/ masking)
	IP Fragment	NO	NO
	IPX Class of Service	NO	NO
	IPX Packet Type	NO	NO
	IPX Network Source/ Destination/Bilateral	NO	NO
	IPX Socket Source/ Destination/Bilateral	NO	NO
	ICMP	NO	NO
	IP Time to Live (TTL)	NO	NO
Layer 4	IP UDP Port Source/ Destination/Bilateral	Permit/Deny Only (port range)	YES (port range)
	IP TCP Port Source/ Destination/Bilateral	Permit/Deny Only (port range)	YES (port range)
	IP UDP Port Source/ Destination/Bilateral Range	Permit/Deny Only	YES
	IP TCP Port Source/ Destination/Bilateral Range	Permit/Deny Only	YES
Layer 7	Application	NO	NO

Rule Support B2/C2/D2 and B3/C3/G3/B5/C5

		B2/C2/D2(1)		B3/C3/G3/B5/C5(1)	
		Access Control	**CoS**	**Access Control**	**CoS**
Layer 2	Ethertype	Permit/Deny/VLAN (2)	YES	Permit/Deny/VLAN	YES
	DSAP/SSAP	NO	NO	NO	NO
	MAC Address Source/ Destination/Bilateral	Permit/Deny Only (MAC masking)	YES (MAC masking)	Permit/Deny Only (MAC masking)	YES (MAC masking)
	VLAN ID	NO	NO	NO	NO
	Priority	NO	NO	NO	NO
Layer 3	IP Type of Service	Permit/Deny Only	YES	Permit/Deny Only	YES
	IP Protocol Type	Permit/Deny Only	YES	Permit/Deny Only	YES
	IP Address Source/ Destination/Bilateral	Permit/Deny Only (IP masking)	YES (IP masking)	Permit/Deny Only (IP masking)	YES (IP masking)
	IP Socket Source/ Destination/Bilateral	Permit/Deny Only (port w/ masking)	YES (port w/ masking)	Permit/Deny Only (port w/ masking)	YES (port w/ masking)
	IP Fragment	NO	NO	NO	NO
	IPX Class of Service	NO	NO	NO	NO
	IPX Packet Type	NO	NO	NO	NO
	IPX Network Source/ Destination/Bilateral	NO	NO	NO	NO
	IPX Socket Source/ Destination/Bilateral	NO	NO	NO	NO
	ICMP	Permit/Deny Only (range)	YES (range)	NO	NO
	IPv6 Address Destination	NO	NO	YES(3)	YES(3)
	IPv6 Socket Source/ Destination/Bilateral	NO	NO	NO	NO
	IPv6 Flow Label	NO	NO	NO	NO
	ICMPv6	NO	NO	Deny Only(4)	NO
	IP Time to Live (TTL)	NO	NO	NO	NO
Layer 4	IP UDP Port Source/ Destination/Bilateral	Permit/Deny Only (port range)	YES (port range)	Permit/Deny Only (port range)	YES (port range)
	IP TCP Port Source/ Destination/Bilateral	Permit/Deny Only (port range)	YES (port range)	Permit/Deny Only (port range)	YES (port range)
	IP UDP Port Source/ Destination/Bilateral Range	Permit/Deny Only	YES	Permit/Deny Only	YES
	IP TCP Port Source/ Destination/Bilateral Range	Permit/Deny Only	YES	Permit/Deny Only	YES
Layer 7	Application	NO	NO	NO	NO

[1]If Policy support is enabled.
[2]VLAN support varies depending on versions. See your firmware release notes for more information.
[3]Supported on B5/C5 devices running firmware version 6.81.xx and higher. This rule support must be enabled via

the following CLI command: "set policy capability ipv6dest enable". If it is not enabled, the rule will be removed from Policy Manager during Enforce.
[4]Supported on B5/C5 devices running firmware version 6.81.xx and higher. Supports only Router Advertisement type.

Rule Support Summit 440G2/620

		Summit 440G2/620	
		Access Control	**CoS**
Layer 2	Ethertype	Permit/Deny (Ethertype w/ masking)	YES (Ethertype w/ masking)
	DSAP/SSAP	NO	NO
	MAC Address Source/ Destination/Bilateral	NO	NO
	VLAN ID	NO	NO
	Priority	NO	NO
Layer 3	IP Type of Service	Permit/Deny (TOS w/ masking)	YES (TOS w/ masking)
	IP Protocol Type	Permit/Deny (Protocol w/ masking)	YES (Protocol w/ masking)
	IP Address Source/ Destination/Bilateral	Permit/Deny (IP w/ masking)	YES (IP w/ masking)
	IP Socket Source/ Destination/Bilateral	YES	YES
	IP Fragment	Permit/Deny	YES
	IPX Class of Service	NO	NO
	IPX Packet Type	NO	NO
	IPX Network Source/ Destination/Bilateral	NO	NO
	IPX Socket Source/ Destination/Bilateral	NO	NO
	ICMP	NO	NO
	IPv6 Address Destination	NO	NO
	IPv6 Socket Source/ Destination/Bilateral	NO	NO
	IPv6 Flow Label	NO	NO
	ICMPv6	NO	NO
	IP Time to Live (TTL)	Permit/Deny	YES
Layer 4	IP UDP Port Source/ Destination/Bilateral	Permit/Deny (IP w/ masking)	YES (IP w/ masking)
	IP TCP Port Source/ Destination/Bilateral	Permit/Deny (IP w/ masking)	YES (IP w/ masking)
	IP UDP Port Source/ Destination/Bilateral Range	Permit/Deny (IP w/ masking)	YES (IP w/ masking)
	IP TCP Port Source/ Destination/Bilateral Range	Permit/Deny (IP w/ masking)	YES (IP w/ masking)
Layer 7	Application	NO	NO

Rule Support Summit 450G2/460G2/670G2/770G2

		Summit 450G2/460G2/670G2/770G2	
		Access Control	**CoS**
Layer 2	Ethertype	Permit/Deny (Ethertype w/ masking)	YES (Ethertype w/ masking)
	DSAP/SSAP	NO	NO
	MAC Address Source/ Destination/Bilateral	Permit/Deny (MAC w/ masking)	YES (MAC w/ masking)
	VLAN ID	NO	NO
	Priority	NO	NO
Layer 3	IP Type of Service	Permit/Deny (TOS w/ masking)	YES (TOS w/ masking)
	IP Protocol Type	Permit/Deny (Protocol w/ masking)	YES (Protocol w/ masking)
	IP Address Source/ Destination/Bilateral	Permit/Deny (IP w/ masking)	YES (IP w/ masking)
	IP Socket Source/ Destination/Bilateral	YES(1)	YES(1)
	IP Fragment	Permit/Deny	YES
	IPX Class of Service	NO	NO
	IPX Packet Type	NO	NO
	IPX Network Source/ Destination/Bilateral	NO	NO
	IPX Socket Source/ Destination/Bilateral	NO	NO
	ICMP	NO	NO
	IPv6 Address Destination	Permit/Deny (IP w/ masking)	YES (IP w/ masking)
	IPv6 Socket Source/ Destination/Bilateral	NO	NO
	IPv6 Flow Label	NO	NO
	ICMPv6	NO	NO
	IP Time to Live (TTL)	Permit/Deny	YES
Layer 4	IP UDP Port Source/ Destination/Bilateral	Permit/Deny (IP w/ masking)	YES (IP w/ masking)
	IP TCP Port Source/ Destination/Bilateral	Permit/Deny (IP w/ masking)	YES (IP w/ masking)
	IP UDP Port Source/ Destination/Bilateral Range	Permit/Deny (IP w/ masking)	YES (IP w/ masking)
	IP TCP Port Source/ Destination/Bilateral Range	Permit/Deny (IP w/ masking)	YES (IP w/ masking)
Layer 7	Application	NO	NO

[1]Supported on Summit devices running firmware version 16.1.2.xx and higher. Firmware not supporting these rules displays event log message on enforce indicating firmware does not support IP Socket Rules.

Rule Support I3

		I3	
		Access Control	**CoS**
Layer 2	Ethertype	Permit/Deny/VLAN	YES
	DSAP/SSAP	NO	NO
	MAC Address Source/ Destination/Bilateral	NO	NO
	VLAN ID	NO	NO
	Priority	NO	NO
Layer 3	IP Type of Service	Permit/Deny Only	YES
	IP Protocol Type	Permit/Deny Only	YES
	IP Address Source/ Destination/Bilateral	Permit/Deny Only (IP masking)	YES (IP masking)
	IP Socket Source/ Destination/Bilateral	Permit/Deny Only (port w/ masking)	YES (port w/ masking)
	IP Fragment	NO	NO
	IPX Class of Service	NO	NO
	IPX Packet Type	NO	NO
	IPX Network Source/ Destination/Bilateral	NO	NO
	IPX Socket Source/ Destination/Bilateral	NO	NO
	ICMP	NO	NO
Layer 4	IP UDP Port Source/ Destination/Bilateral	Permit/Deny Only (port range)	YES (port range)
	IP TCP Port Source/ Destination/Bilateral	Permit/Deny Only (port range)	YES (port range)
	IP UDP Port Source/ Destination/Bilateral Range	Permit/Deny Only	YES
	IP TCP Port Source/ Destination/Bilateral Range	Permit/Deny Only	YES
Layer 7	Application	NO	NO

Rule Support K-Series and S-Series

		K-Series/S-Series	
		Access Control	**CoS**
Layer 2	Ethertype	Permit/Deny/VLAN (range)	YES (range)
	DSAP/SSAP	Permit/Deny/VLAN (DSAP/SSAP masking)	YES (DSAP/SSAP masking)
	MAC Address Source/ Destination/Bilateral	Permit/Deny/VLAN (MAC masking)	YES (MAC masking)
	VLAN ID	Permit/Deny/VLAN (VLAN ID range)	YES (VLAN ID range)
	Priority	Permit/Deny/VLAN	YES
Layer 3	IP Type of Service	Permit/Deny/VLAN	YES
	IP Protocol Type	Permit/Deny/VLAN (range)	YES (range)
	IP Address Source/ Destination/Bilateral	Permit/Deny/VLAN (IP masking)	YES (IP masking)
	IP Socket Source/ Destination/Bilateral	Permit/Deny/VLAN (port w/ masking)	YES (port w/ masking)
	IP Fragment	Permit/Deny/VLAN	YES
	IPX Class of Service	Permit/Deny/VLAN (port range)	YES (port range)
	IPX Packet Type	Permit/Deny/VLAN (port range)	YES (port range)
	IPX Network Source/ Destination/Bilateral	Permit/Deny/VLAN (port range)	YES (port range)
	IPX Socket Source/ Destination/Bilateral	Permit/Deny/VLAN (port range)	YES (port range)
	ICMP	Permit/Deny/VLAN	YES
	IPv6 Address Source/ Destination/Bilateral	7.31.xx and later Permit/Deny/VLAN (IP masking)	7.31.xx and later YES (IP masking)
	IPv6 Socket Source/ Destination/Bilateral	7.31.xx and later Permit/Deny/VLAN (port w/ masking)	7.31.xx and later YES (port w/ masking)
	IPv6 Flow Label	7.31.xx and later Permit/Deny/VLAN	7.31.xx and later YES
	ICMPv6	7.31.xx and later Permit/Deny/VLAN	7.31.xx and later YES
	IP Time to Live (TTL)	Permit/Deny/VLAN	YES

		K-Series/S-Series	
		Access Control	**CoS**
Layer 4	IP UDP Port Source/ Destination/Bilateral	Permit/Deny/VLAN (port range or IP w/ masking)	YES (port range or IP w/ masking)
	IP TCP Port Source/ Destination/Bilateral	Permit/Deny/VLAN (port range or IP w/ masking)	YES (port range or IP w/ masking)
	IP UDP Port Source/ Destination/Bilateral Range	Permit/Deny/VLAN	YES
	IP TCP Port Source/ Destination/Bilateral Range	Permit/Deny/VLAN	YES
Layer 7	Application	8.02.xx and later Permit/Deny/VLAN	8.02.xx and later YES

Rule Support ExtremeWireless Controller

		ExtremeWireless Controller	
		Access Control	**CoS**
Layer 2	Ethertype	8.31.xx and later Permit/Deny/VLAN	8.31.xx and later YES
	DSAP/SSAP	NO	NO
	MAC Address Source/ Destination/Bilateral	8.31.xx and later Permit/Deny/VLAN	8.31.xx and later YES
	VLAN ID	NO	NO
	Priority	8.01.xx and later Permit/Deny/VLAN(3)	8.01.xx and later YES
Layer 3	IP Type of Service	8.01.xx and later Permit/Deny/VLAN(3)	8.01.xx and later YES
	IP Protocol Type(1)	Permit/Deny/VLAN(3)	8.01.xx and later YES
	IP Address Source/ Bilateral	8.01.xx and later Permit/Deny/VLAN(3)	8.01.xx and later YES
	IP Address Destination	Permit/Deny/VLAN(3)	8.01.xx and later YES
	IP Socket Source/ Bilateral	8.01.xx and later Permit/Deny/VLAN(3)	8.01.xx and later YES
	IP Socket Destination	Permit/Deny/VLAN(3)	8.01.xx and later YES
	IP Fragment	NO	NO
	IPX Class of Service(2)	NO	NO
	IPX Packet Type(2)	NO	NO
	IPX Network Source/ Destination/Bilateral(2)	NO	NO
	IPX Socket Source/ Destination/Bilateral(2)	NO	NO
	ICMP	Permit/Deny/VLAN(3)	8.01.xx and later YES
	IP Time to Live (TTL)	NO	NO

		ExtremeWireless Controller	
		Access Control	**CoS**
Layer 4	IP UDP Port Source/ Bilateral	8.01.xx and later Permit/Deny/VLAN(3)	8.01.xx and later YES
	IP UDP Port Destination	Permit/Deny/VLAN(3)	8.01.xx and later YES
	IP TCP Port Source/ Bilateral	8.01.xx and later Permit/Deny/VLAN(3)	8.01.xx and later YES
	IP TCP Port Destination	Permit/Deny/VLAN(3)	8.01.xx and later YES
	IP UDP Port Source/ Bilateral Range	8.01.xx and later Permit/Deny/VLAN(3)	8.01.xx and later YES
	IP UDP Port Destination Range	Permit/Deny/VLAN(3)	8.01.xx and later YES
	IP TCP Port Source/ Bilateral Range	8.01.xx and later Permit/Deny/VLAN(3)	8.01.xx and later YES
	IP TCP Port Destination Range	Permit/Deny/VLAN(3)	8.01.xx and later YES
Layer 7	Application	9.12.xx and later Permit/Deny/VLAN(3)	9.12.xx and later YES

[1]Not all IP Protocols are supported for the ExtremeWireless Controller. Supported IP Protocols for this rule type are: ICMP, TCP, UDP, GRE, ESP, AH.
[2]The ExtremeWireless Controller automatically blocks all IPX traffic, as it is unsuited to wireless transmission.
[3] Contain to VLAN is supported on 8.31.xx and later only.

Inventory Manager Firmware Support

The following table shows Inventory Manager feature support for hardware products and firmware versions.

	Firmware Version				
Product	**Download Firmware**	**Download Config Template**	**Save Archive**	**Restore Archive**	**Reset Device**
7100-Series	8.42.xx	8.42.xx	8.42.xx	8.42.xx	8.42.xx
800-Series(1)	1.02.01.xx	Not Supported	1.02.01.xx	1.02.01.xx	Not Supported
A2	3.03.xx	3.03.xx	3.03.xx	3.03.xx	3.03.xx
A4	6.81.xx	6.81.xx	6.81.xx	6.81.xx	6.81.xx
B2	4.02.xx	4.02.xx	4.02.xx	4.02.xx	4.02.xx
B3/C3/G3/I3	6.61.xx	6.61.xx	6.61.xx	6.61.xx	6.61.xx
B5/C5	6.81.xx	6.81.xx	6.81.xx	6.81.xx	6.81.xx
D2	6.03.xx	6.03.xx	6.03.xx	6.03.xx	6.03.xx
ExtremeWireless Controller	10.01.xx	Not Supported	10.01.xx	10.01.xx	10.01.xx
K-Series	8.42.xx	8.42.xx	8.42.xx	8.42.xx	8.42.xx
S-Series	8.42.xx	8.42.xx	8.42.xx	8.42.xx	8.42.xx
BlackDiamond Series(1)(2)	15.3.x	Not Supported	15.3.x	15.3.x	15.3.x
E4G Series (1)(2)	15.3.x	Not Supported	15.3.x	15.3.x	15.3.x
Summit Series(1)(2)	15.3.x	15.7.x	15.3.x	15.3.x	15.3.x

[1]To perform these functions, Inventory Manager uses a script that requires accurate CLI credentials.
[2]Utilizes Extreme Control Center script functionality. VR-Default is the default used in Controlled by device type. If VR-Mgmt required, use MIB and Script Overrides (ExtremeXOS-TFTP (VR-Mgmt))

ACL Manager Firmware Support

ACL Manager is a Extreme Control Center Console tool that lets you efficiently manage the Access Control Lists (ACLs) on your network routers. ACL Manager supports the following Extreme Networks hardware products and firmware versions:

Product	Firmware Version
K-Series	7.31 and later
S-Series	7.11 and later

Automated Security Manager Firmware Support

Devices that support Static Policies must be able to discard traffic at the role level and apply a Quarantine role that is set up to discard traffic. Refer to Policy Manager Firmware Support for policy support information for specific device types.

OneView Firmware Support

OneView requires ExtremeWireless Controller firmware version 8.01 or later. Earlier firmware versions are not supported.

ExtremeWireless Firmware Support

OneView and ExtremeWireless can be used to monitor and configure ExtremeWireless Controllers running firmware version 8.01 or later.

Extreme Networks Support

If you require assistance, contact Extreme Networks Global Technical Assistance Center using one of the following methods.

Web	www.extremenetworks.com/support/
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-603-952-5000 For the Extreme Networks Support phone number in your country: www.extremenetworks.com/support/contact/
Email	support@extremenetworks.com

04/2016
PN: 9034973