

# Extreme Management Center Firmware Support for Legacy Products

---

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

- [NAC Manager Firmware Support](#)
- [Policy Manager Firmware Support](#)

The following legacy Enterasys products are included in this document:

A2	B3/C3/G3
B2	C2

For firmware support information for current Extreme Networks devices, see the Extreme Management Center Firmware Support document.

## NAC Manager Firmware Support

NAC Manager supports the following legacy Enterasys devices and firmware versions:

Product	Firmware Version
A2	3.02.xx 3.03.xx
B2 and B2/B3 (Mixed Stack)	4.00.xx 4.01.xx 4.02.xx
B3/C3 (Standalone)/ G3	6.03.xx 6.42.xx 6.61.xx
C2 and C2/C3 (Mixed Stack)	5.00.xx 5.01.xx 5.02.xx

# Policy Manager Firmware Support

[Section 1](#) lists the legacy Enterasys products and firmware versions supported by Policy Manager.

[Section 2](#) lists the Policy Manager feature sets for the legacy products.

[Section 3](#) lists the Access Control and CoS Classification Rule Support for the legacy products.

## Section 1: Devices/Firmware Versions Supported

This table displays the legacy Enterasys products and firmware versions supported by Policy Manager.

Product	Firmware Version
A2	3.02.xx
	3.03.xx
B2	4.00.xx
	4.01.xx
	4.02.xx
B3/C3/G3	6.03.xx
	6.42.xx
	6.61.xx
C2	5.00.xx
	5.01.xx
	5.02.xx

## Section 2: Policy Manager Feature Support

- [A2](#)
- [B2](#)
- [B3/C3/G3](#)
- [C2](#)

### Feature Support A2

Functionality	A2 Firmware Version	
	3.02.xx	3.03.xx
	Authentication Support	X
802.1X	X	
MAC	X	
MAC Mask	X	
Web-Based	-	
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	-	
Policy-based VLAN Egress	-	
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(1)	

	A2 Firmware Version
Functionality	3.02.xx 3.03.xx
MAC Locking	X
ToS/DSCP Rewrite	-
Anti-Spoofing	-

<sup>1</sup>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 not supported.

### *Feature Support B2*

	B2 Firmware Version
Functionality	4.00.xx(1) 4.01.xx(1) 4.02.xx(1)
Authentication Support	X
802.1X	X(2)
MAC	X(2)
MAC Mask	X
Web-Based	X(2)
CEP	-
Quarantine	-
Auto Tracking	-
Global Authentication Settings:	X
Authentication Timeout	X
Current # of Authenticated Users	X
Multi-Users per Port	X(3,4)
RFC3580 VLAN Authorization	X
RFC3580 VLAN Egress	X
RADIUS Support	X
RADIUS Accounting	-
RADIUS Response Mode	X
Priority Support (802.1p)	X
Policy Support	X(2)
Policy-based VLAN Egress	X
Tagged Packet VLAN to Role Mapping	X(5)
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	-

	B2 Firmware Version
	4.00.xx(1)
	4.01.xx(1)
<b>Functionality</b>	4.02.xx(1)
Rate Limiting	X(6)
MAC Locking	X
ToS/DSCP Rewrite	X(7)
Anti-Spoofing	-

<sup>1</sup>This firmware version supports mixed-stacking with B3 devices.

<sup>2</sup>Can be enabled at the device-level and port-level, but there can be only one active session at a time.

<sup>3</sup>One authenticated user and one VoIP phone (with VLAN tagged VoIP traffic) per port.

<sup>4</sup>Dynamic MAC locking supported. Static MAC Locking supported only if Policy support is enabled.

<sup>5</sup>This feature does 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.

<sup>6</sup>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.

<sup>7</sup>If Policy support is enabled.

### *Feature Support B3/C3/G3*

	B3/C3/G3 Firmware Version
	6.03.xx
	6.42.xx
<b>Functionality</b>	6.61.xx
Authentication Support	X
802.1X	X
MAC	X
MAC Mask	X
Web-Based	X
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(2)
RFC3580 VLAN Egress	X
RADIUS Support	X
RADIUS Accounting	-
RADIUS Response Mode	X
Priority Support (802.1p)	X

	B3/C3/G3 Firmware Version
Functionality	6.03.xx 6.42.xx 6.61.xx
Policy Support	X(3)
Policy-based VLAN Egress	X
Tagged Packet VLAN to Role Mapping	X(4)
Authentication-based VLAN to Role Mapping	X(5)
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(2)
Anti-Spoofing	-

<sup>1</sup>On B3, only if Policy support is enabled. On G3, maximum eight authenticated users per port.

<sup>2</sup>On B3, up to three multiple RFC3580 users per Gigabit port. On C3, up to six multiple RFC3580 users per Gigabit port. On G3, for 6.03.xx, RFC3580 is only supported for 802.1X authentication.

<sup>3</sup>On B3, only if Policy support is enabled. On C3 and G3, see Firmware Release Notes for details.

<sup>4</sup>On B3 and C3, this feature does 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. On G3, only one device-level mapping is supported.

<sup>5</sup>On G3, supports multiple device-level mapping with a maximum of eight per port in effect at one time.

<sup>6</sup>For Role-Based Rate Limiting, any rate limit specified by a Class of Service in a rule is 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 C2

Functionality	C2 Firmware Version			
	5.00.xx(1)	5.01.xx(1)	5.02.xx(1)	
	Authentication Support	X		
	802.1X	X(2)		
MAC	X(2)			
MAC Mask	X			
Web-Based	X(2)			
CEP	-			
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(4)			
RFC3580 VLAN Egress	X			
RADIUS Support	X			
RADIUS Accounting	-			
RADIUS Response Mode	X			
Priority Support (802.1p)	X			
Policy Support	X(5)			
Policy-based VLAN Egress	X			
Tagged Packet VLAN to Role Mapping	X(6)			
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(7)			
MAC Locking	X			
ToS/DSCP Rewrite	X			
Anti-Spoofing	-			

<sup>1</sup>This firmware version supports mixed-stacking with C3 devices.

<sup>2</sup>Can be enabled at the device-level and port-level, but there can be only one active session at a time.

<sup>3</sup>One authenticated user and one VoIP phone (with VLAN tagged VoIP traffic) per port.

<sup>4</sup>Up to six multiple RFC3580 users per Gigabit port (C2Gxxx-xx devices version 5.01.01.0049 and later only).

<sup>5</sup>See Firmware Release Notes for details.

<sup>6</sup>This feature does 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. Firmware version 5.00.xx also supports one port-level mapping per port.

<sup>7</sup>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.



## Section 3: Access Control/CoS Classification Rule Support

- [B2/C2 and B3/C3/G3](#)
- [A2](#)

### Rule Support B2/C2 and B3/C3/G3

		B2/C2/D2(1)		B3/C3/G3(1)	
		Access Control	CoS	Access Control	CoS
<b>Layer 2</b>	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)
	VLANID	NO	NO	NO	NO
	Priority	NO	NO	NO	NO
<b>Layer 3</b>	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	NO	NO
	IPv6 Socket Source/ Destination/Bilateral	NO	NO	NO	NO
	IPv6 Flow Label	NO	NO	NO	NO
	ICMPv6	NO	NO	NO	NO
IP Time to Live (TTL)	NO	NO	NO	NO	

		B2/C2/D2(1)		B3/C3/G3(1)	
		Access Control	CoS	Access Control	CoS
<b>Layer 4</b>	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
<b>Layer 7</b>	Application	NO	NO	NO	NO

<sup>1</sup>If Policy support is enabled.

<sup>2</sup>VLAN support varies depending on versions. See your firmware release notes for more information.

## Devices That Do Not Support Policy Manager Rules

Device	Access Control/CoS Classification Rule Support
A2	Not Supported

## 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/](http://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/enterasys-support/contact/](http://www.extremenetworks.com/support/enterasys-support/contact/)

---

Email [support@extremenetworks.com](mailto:support@extremenetworks.com)

---

3/2018

PN: 9035429

Content Subject to Change Without Notice