Extreme Visibility Manager Release Notes

6.1.2

9037157-02 Rev AA
January 2022

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

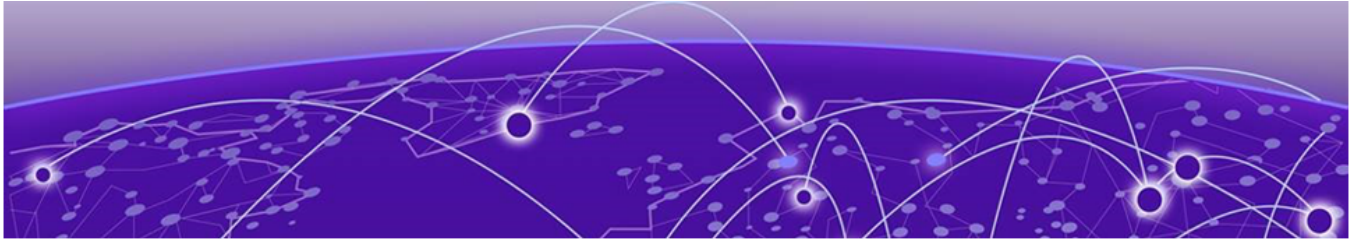

Table of Contents

Release Notes....4

New In This Release....4

Supported Devices and Software....4

Known Limitations....5

Defects Closed With Code Changes....7

Open Defects....8

Help and Support....21

Subscribe to Product Announcements....22

Release Notes

New In This Release on page 4
Supported Devices and Software on page 4
Known Limitations on page 5
Defects Closed With Code Changes on page 7
Open Defects on page 8
Help and Support on page 21

Extreme Visibility Manager, a Kubernetes-based microservices application, provides centralized device and policy management as part of the Extreme Visibility solution.

New In This Release

Extreme Visibility Manager version 6.1.2 resolves several issues.

For more information, see Defects Closed With Code Changes on page 7.

Supported Devices and Software

Extreme Visibility Manager supports several devices and their software.

Table 1: Supported devices and software

Visibility Manager Version	Supported Device	Supported Device Software
6.1.2	Extreme 9920	Extreme 9920 software with the NPB application, versions: • 21.1.1.0 • 21.1.1.1 • 21.1.2.0
6.1.1	Extreme 9920	Extreme 9920 software with the NPB application, version 21.1.1.0.
6.0.0	Extreme 9920	Extreme 9920 software with the NPB application, version 21.1.0.x.
6.1.x	ExtremeRouting MLX series	NetIron 6.3.00d
6.1.2	ExtremeSwitching SLX 9140	• SLX-OS 18s.1.03a • SLX-OS 18s.1.03b • SLX-OS 18s.1.03c
6.1.1	ExtremeSwitching SLX 9140	SLX-OS 18s.1.03c

Table 1: Supported devices and software (continued)

Visibility Manager Version	Supported Device	Supported Device Software
6.1.2	ExtremeSwitching SLX 9240	• SLX-OS 18s.1.03a • SLX-OS 18s.1.03b • SLX-OS 18s.1.03c
6.1.1	ExtremeSwitching SLX 9240	SLX-OS 18s.1.03c

Known Limitations

Note the following caveats for this release of Extreme Visibility Manager.

LAG created when port channel deployment fails

Any changes to Visibility Manager configuration are reverted when a port channel deployment fails. However, even when deployment fails, a link aggregation group (LAG) is created on the device. The LAG is immediately deleted, but you will see the creation and deletion of a LAG in logs for the device.

Egress group configuration cannot be updated during migration

During the migration of MLX configuration to an Extreme 9920 device, you cannot change the configuration of an egress group. After migration is complete, you can change the configuration on the 9920, including the mapping of multiple egress to an egress group.

MLX UDA profile must be associated with an ingress group if the policy contains a UDA match

(MLX only) When you create an ingress group and associate it with an ingress policy, you must also associate the group with a UDA profile if the ingress policy contains a UDA match.

This instruction is documented in the *Extreme Visibility Manager Administration and User Guide, 6.1.0* but not in the Visibility Manager online help.

Firmware upgrade requires an absolute path to image locations

In the **Absolute Path** field, enter the complete file path to the location of the firmware image. The following are sample file paths for the various supported devices.

9920 (absolute path to the binary file): `/root/TierraOS-<version>-NPB.bin`

SLX (absolute directory path where supported image files are located): `/root/slxos18s.1.03/slxos18s.1.03a`

MLX (path to the manifest file): `XMR-MLX/MLX_npb_06200_mnf.txt`

This instruction is documented in the *Extreme Visibility Manager Administration and User Guide, 6.1.0* but not in the Visibility Manager online help.

A device can be managed by only one instance of VM

Before adding a device, ensure that it is not managed by any other instance of Visibility Manager.

This instruction is documented in the *Extreme Visibility Manager Administration and User Guide, 6.1.0* but not in the Visibility Manager online help.

Listener policy byte count is incorrect when truncation is enabled

On the Extreme 9920 device, the byte count for truncated packets is the actual byte count seen by the egress ACL before truncation.

LACP LAG is not supported for Extreme 9920 devices

Although the option to select LACP LAG appears in the Create Port Channel page, the option is grayed out. Only static LAG is supported.

Only one region is supported

This release supports the creation and management of only one region.

Defects Closed With Code Changes

The following defects were closed with code changes in this release of Extreme Visibility Manager.

Parent Defect ID:	XVM-3017	Issue ID:	XVM-3017
Severity:	S3 - Moderate		
Product:	XVM	Reported in Release:	XVM 6.1.0
Summary:	Port channel reconciliation not happening for NGNPB with version 21.1.2.0		

Parent Defect ID:	XVM-3024	Issue ID:	XVM-3024
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.1
Summary:	Ingress group stats not populated in XVM dashboard for 9920		

Parent Defect ID:	XVM-3025	Issue ID:	XVM-3025
Severity:	S3 - Moderate		
Product:	XVM	Reported in Release:	XVM 6.1.1
Summary:	Card view not in sync with the consolidated view for Ingress group with IP address in XVM		

Parent Defect ID:	XVM-3026	Issue ID:	XVM-3026
Severity:	S3 - Moderate		
Product:	XVM	Reported in Release:	XVM 6.1.1
Summary:	Route Map sequence number not sorted for 9920 policy in XVM		

Parent Defect ID:	XVM-3030	Issue ID:	XVM-3030
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.1
Summary:	[VZW-CAT]:Error for device in XVM after image upgrade from XVM		

Parent Defect ID:	XVM-3031	Issue ID:	XVM-3031
	S3 - Moderate		

Parent Defect ID:	XVM-3031	Issue ID:	XVM-3031
Severity:			
Product:	XVM	Reported in Release:	XVM 6.1.1
Summary:	port channel creation is restricted with an error message pointing to MTU default value on Freedom SLX device		

Parent Defect ID:	XVM-3032	Issue ID:	XVM-3032
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.2
Summary:	Breakout ports not reconciled for mirror in XVM		

Parent Defect ID:	XVM-3033	Issue ID:	XVM-3033
Severity:	S1 - Critical		
Product:	XVM	Reported in Release:	XVM 6.1.2
Summary:	XVM 6.1.2 - XVM shows blank on clicking "Add ACL" or "Add Policy" in GUI		

Parent Defect ID:	XVM-3034	Issue ID:	XVM-3034
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.2
Summary:	NGNPB-Platform: Service chain configuration refresh hangs on deleting egress object		

Parent Defect ID:	XVM-3036	Issue ID:	XVM-3036
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.2
Summary:	NGNPB-Platform: On XVM, Firmware upgrade status shows as active with wrong absolute path instead of error		

Open Defects

The following defects are open in this release of Extreme Visibility Manager.

Parent Defect ID:	XVM-1224	Issue ID:	XVM-1224
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 0.1.0
Symptom:	During export configuration from MLX/SLX to 9920, policy name and match names displayed which are given by the XVM instead of the actual name.		

Parent Defect ID:	XVM-1224	Issue ID:	XVM-1224
Condition:	During export configuration from MLX/SLX to 9920, policy name and match names displayed which are given by the XVM instead of the actual name.		
Workaround:	NA		
Recovery:	NA		

Parent Defect ID:	XVM-1970	Issue ID:	XVM-1970
Severity:	S3 - Moderate		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	Demand reconciliation is not working		
Condition:	one of regional node is rebooted		
Workaround:	Wait for the rebooted regional node join to patroni cluster		

Parent Defect ID:	XVM-2125	Issue ID:	XVM-2125
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	Login to XVM GUI gives "Invalid Username" even when we give right credentials.		
Condition:	Happens when regional VM reboots.		

Parent Defect ID:	XVM-2125	Issue ID:	XVM-2125
Workaround:	1. Always keep regional VM which is Leader running, Leader VM can be identified by below command on any regions VMs. [root@ ~]# patronictl -c /opt/app/patroni/etc/postgresql.yml list postgres + Cluster: postgres (6969515509939729866) ---------- MemberHostRoleStateTLLag in MB ----------+ pg_10.37.136.16210.37.136.162 running20 pg_10.37.136.16310.37.136.163Leaderrunning pg_10.37.136.16410.37.136.164 running80 2. Check on monitoring alerts for Patroni "PostgreSQLReplicationUnhealthy" if so recover it soon with recovery mechanism provided.		
Recovery:	1. Power on Leader node 2. backup old data folder on problematic regional nodes. "mv /var/lib/pgsql/12/data /var/lib/pgsql/12/data_org 3. execute below command "pg_basebackup -h <Leader regional IP> -U cmon_replication -Xs -P -R -D /var/lib/postgresql/12/data" 4 Execute below command and wait for State to change from "creating Replica" to running. [root@ ~]# patronictl -c /opt/app/patroni/etc/postgresql.yml list postgres + Cluster: postgres (6969515509939729866) ---------- Member Host Role State TL Lag in MB ----------+ pg_10.37.136.162 10.37.136.162 running 2 0 pg_10.37.136.163 10.37.136.163 Leader running pg_10.37.136.164 10.37.136.164 running 8 0		

Parent Defect ID:	XVM-2130	Issue ID:	XVM-2130
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	NGNPB configuration details are not displayed on XVM UI after migrating policy, rules from MLX/SLX devices.		
Condition:	When ACL rules, policy configuration of source device has syntax/semantic conflicts with NGNPB accepted configuration.		
Workaround:	Refresh configuration of the NGNPB device again to display the details.		

Parent Defect ID:	XVM-2142	Issue ID:	XVM-2142
Severity:	S3 - Moderate		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	Duplicate port entries are seen in the interface statistics dashboard.		

Parent Defect ID:	XVM-2142	Issue ID:	XVM-2142
Condition:	When the SCS service gets re-initialized, the duplicate entries are seen in the statistics dashboard.		
Workaround:	Refresh the page, new stats entries will be updated correctly.		

Parent Defect ID:	XVM-2162	Issue ID:	XVM-2162
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.0.0
Symptom:	Configuration is reconciled from device and old config is retained after Refresh Configuration (on-demand reconciliation).		
Condition:	1. When refresh configuration is performed after rebooting the device. 2. Applying default config on device, this reboots the device.		
Workaround:	Wait for few minutes (~4-5) before executing refresh configuration. This will allow XVM to reconnect to the device services. If the configs are still persists, please delete and add the device from XVM.		

Parent Defect ID:	XVM-2385	Issue ID:	XVM-2385
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	Additional "/" character is added when the name of object contain the "/" character		
Condition:	When the name contains "/" character in the object name		
Workaround:	Avoid the "/" character in the current release and use other character like "_"		
Recovery:	Not applicable		

Parent Defect ID:	XVM-2444	Issue ID:	XVM-2444
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	IPv6 match rule mask edit not working		
Condition:	When a rule with XX::XX/prefix is reconciled for MLXe and if the user updates the mask value for either for source or destination address, same is not reflected on to device and will retain the old mask value.		
Workaround:	To update mask value of XX::XX/prefix math, delete the match and add match with new mask value		
Recovery:	Perform the refresh configuration to sync the configuration b/n MLX and XVM.		

Parent Defect ID:	XVM-2452	Issue ID:	XVM-2452
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.0

Parent Defect ID:	XVM-2452	Issue ID:	XVM-2452
Symptom:	If ACL contains the IPv4 address in the IPv6 address, those ACLs are not reconciled by the XVM		
Condition:	IPv4 address are represented as the IPv6 address		
Workaround:	Provide only ipv6 and ipv4 address separately. IPv4 address should not be given as IPv6 address.		
Recovery:	not applicable		

Parent Defect ID:	XVM-2456	Issue ID:	XVM-2456
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	When multiple sequence number rules with different combination of prefix are present, the rule update is failing for IPv6 matches		
Condition:	Multiple prefix combination present in the single rule for IPv6 ACL match		
Workaround:	None		
Recovery:	Need to perform the refresh configuration to sync the configuration from device to XVM		

Parent Defect ID:	XVM-2591	Issue ID:	XVM-2591
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	MLX device is stuck in reconciliation state or device configuration is not reconciled during refresh configuration		
Condition:	Refresh configuration operation performed when device is being rebooted.		
Workaround:	- Wait for device reboot to complete and then perform refresh configuration. - Delete and add the device again from XVM UI.		

Parent Defect ID:	XVM-2599	Issue ID:	XVM-2599
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	For MLX devices, route-map action is not updated with tvf-domain or vlan id.		
Condition:	When route-map name has special characters like "\".		
Workaround:	Create route-maps with out special characters.		

Parent Defect ID:	XVM-2601	Issue ID:	XVM-2601
	S2 - Major		

Parent Defect ID:	XVM-2601	Issue ID:	XVM-2601
Severity:			
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	Few Pod restarts seen across regional VMs		
Condition:	This happens when regional VMs are rebooted randomly.		
Workaround:	Avoid rebooting multiple VMs at a single time.		
Recovery:	1. Login to mongo db pod using below command and check mongo members if all have properly catagorised as Primary or Secondary a. # kubectl exec -it ms-db-0 -n xvm -- /bin/sh //On ControlPlane b. mongo c. rs.status() //Check for “stateStr” it should be “Primary” or “Secondary” 2. If any member is Unknown or have multiple primary and is not recovering we may have to delete underlying persistent volume and restart that replica(Secondary). a. In the replica (or one of primary if dual primary is seen) rm -fr /mnt/persistent-cs-volume-* b. Restart ms-db-* instance for the replica (kubectl get pods -n xvm -o wide , will mention which instance runs on which node) c. Continue on other replica. d. cd /etc/xvm/controlplane_node_binaries e. ./loadPodsInControlPlaneNode.sh		

Parent Defect ID:	XVM-2674	Issue ID:	XVM-2674
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	Egress object column shows number of ports updated even though it failed when we add a lag to egress object whose port are already part of the egress object in MLXe.		
Condition:	Add a lag to egress object whose port are already part of the egress object in MLXe		
Workaround:	Error message is displayed in UI notification but egress configuration is not reverted to previous configuration.		
Recovery:	Reloading the UI page reverts egress to previous configuration		

Parent Defect ID:	XVM-2708	Issue ID:	XVM-2708
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	MLXe device does not get discovered		
Condition:	The "enable" prompt is enabled with username and password		
Workaround:	Having default username and password for "enable" prompt on MLXe device		

Parent Defect ID:	XVM-2738	Issue ID:	XVM-2738
	S2 - Major		

Parent Defect ID:	XVM-2738	Issue ID:	XVM-2738
Severity:			
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	For slot configurations, if the list of interfaces are not same in different processor, the interfaces are not removed for the egress truncation		
Condition:	List of interfaces in the slot level truncation contains different set of interfaces in different processor		
Workaround:	Make sure that the interface list contains same names for both processors in the slot configuration for truncation.		
Recovery:	Remove the interface from the both processor which should be removed from the truncation after performing the refresh configuration.		

Parent Defect ID:	XVM-2756	Issue ID:	XVM-2756
Severity:	S3 - Moderate		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	If a port is part of lag and is also configured in the packet slicing slot configuration, and if it is removed, then we may see error and there may be configuration differentiated with XVM and device. Same is true if the lag port is part of the TVF domain		
Condition:	The port which is part of the lag is part of the packet slice or the TVF domain and the port is getting removed		
Workaround:	None		
Recovery:	Refresh configuration of device so that XVM fetch the latest configuration from the device		

Parent Defect ID:	XVM-2793	Issue ID:	XVM-2793
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	Sometimes ports, port-channels are not displayed after performing refresh configuration.		
Condition:	Ports, Port-channels are not shown on XVM UI.		
Workaround:	No work around		
Recovery:	Switch to another tab (dashboard, inventory) and go back to configuration tab or refresh the page to display the ports/port-channels.		

Parent Defect ID:	XVM-2871	Issue ID:	XVM-2871
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.0

Parent Defect ID:	XVM-2871	Issue ID:	XVM-2871
Symptom:	Configuration mismatch seen between XVM and device in case of MLX when loopback is enabled for interface of module for which loopback is not supported.		
Condition:	Enabling the loopback on the interface of module for which loopback is not supported.		
Workaround:	Don't enable loopback from XVM for interface of module for which loopback is not supported.		
Recovery:	Perform the refresh configuration from XVM.		

Parent Defect ID:	XVM-2873	Issue ID:	XVM-2873
Severity:	S3 - Moderate		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	Sometime egress-group is not shown in the XVM for device and need to switch the tab for getting the egress-group configuration		
Condition:	Egress-group and egress are not listed in XVM		
Workaround:	Switch the tab (i.e. go to dashboard tab and come back to configuration tab) to get the egress and egress-group configurations		
Recovery:	Switch the tab (i.e. go to dashboard tab and come back to configuration tab) to get the egress and egress-group configurations		

Parent Defect ID:	XVM-2878	Issue ID:	XVM-2878
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	Device Type count is shown non zero even when all DTVCs are deleted.		
Condition:	Issue happens if Deleting Dtcv Fails due to XVM bad connections with the devices to which dtvc belongs.		
Workaround:	Check Device connectivity		
Recovery:	When DTCV fails re-add DTCV and try delete again.if problem persists need to check logs to recover.		

Parent Defect ID:	XVM-2894	Issue ID:	XVM-2894
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	Policies are not reconciled.		
Condition:	The route-map consists the interface as the nexthop		

Parent Defect ID:	XVM-2894	Issue ID:	XVM-2894
Workaround:	Create the tvf domain or the flood VLAN and provide it as the egress action for the policy rule action		
Recovery:	None		

Parent Defect ID:	XVM-2927	Issue ID:	XVM-2927
Severity:	S3 - Moderate		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	The notification message is not displayed when device discovery failed		
Condition:	When the device discovery request fails due to a connectivity issue		
Workaround:	None		
Recovery:	Rediscover the device after resolving the connectivity issue.		

Parent Defect ID:	XVM-2936	Issue ID:	XVM-2936
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	Removal of one type rules delete complete policy from interfaces		
Condition:	When single instance of the rule (like L2/IPv4/IPv6) gets removed from policy, complete policy is getting deleted from the interface		
Workaround:	Remove/Un-bind the policy from the ingress-group and then remove the rule from policy and then attach/bind the policy to ingress-group		
Recovery:	Remove/un-bind the policy from ingress group and then attach/bind the ingress-group with policy		

Parent Defect ID:	XVM-2939	Issue ID:	XVM-2939
Severity:	S3 - Moderate		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	In XVM the loopback flag is not reflected on the primary port		
Condition:	When loopback is enabled on port-channel/lag for MLXe device, in XVM the loopback flag is not reflected on the primary port		
Workaround:	Perform the refresh configuration after enabling the loopback on the lag or port-channel interface		
Recovery:	Perform the refresh configuration after enabling the loopback on the lag or port-channel interface		

Parent Defect ID:	XVM-2943	Issue ID:	XVM-2943
	S2 - Major		

Parent Defect ID:	XVM-2943	Issue ID:	XVM-2943
Severity:			
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	Ingress-group configuration not migrated from MLX to NGNPB and failure notification shown on UI.		
Condition:	When policy applied in ingress-group is not present on the device.		
Workaround:	- Same ingress-group can be created from XVM. - Retry MLX to NGNPB migration.		

Parent Defect ID:	XVM-2947	Issue ID:	XVM-2947
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	The bulk device deletion failed and the device(s) moved to the error state		
Condition:	Device deletion request having many devices is failing due to response timeout.		
Workaround:	Delete the devices in small batches.		
Recovery:	Select the devices which are in the error state from managed device table and request to delete once again.		

Parent Defect ID:	XVM-2949	Issue ID:	XVM-2949
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	- ingress-group configurations shows primary port of the port-channel. - ingress-group update with port-channel and primary port of the port-channel throws an error.		
Condition:	When a port-channel and primary port of the port-channel are added to ingress-group		
Recovery:	Remove primary port and add the corresponding port-channel to update the ingress-group correctly. Subsequent ingress-group operations should work fine.		

Parent Defect ID:	XVM-2961	Issue ID:	XVM-2961
Severity:	S3 - Moderate		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	Intermittently on firmware upgrade of bulk devices , Firmware upgrade status of few of the devices will result in error state on XVM		

Parent Defect ID:	XVM-2961	Issue ID:	XVM-2961
Condition:	While performing firmware upgrade of bulk devices, Firmware activation failure occurs on device due to broken connection between scp server and device, image checksum error, intermittent connection failure between xvm cluster and device		
Recovery:	Retrigger the firmware upgrade one at a time for devices which are in firmware upgrade error status		

Parent Defect ID:	XVM-2963	Issue ID:	XVM-2963
Severity:	S3 - Moderate		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	Configuration fails to apply on MLX device		
Condition:	Sometimes configuration pushed from XVM to MLX device fails with error "unable to establish connection: ssh: handshake failed: EOF".		
Workaround:	None		
Recovery:	Push the configuration again from the XVM to MLX device.		

Parent Defect ID:	XVM-2972	Issue ID:	XVM-2972
Severity:	S3 - Moderate		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	Loopback flag for port channel is not reconciled		
Condition:	Lag for which loopback flag is enabled which is not deployed		
Workaround:	Deploy the lag for which loopback is enabled		
Recovery:	None		

Parent Defect ID:	XVM-2973	Issue ID:	XVM-2973
Severity:	S3 - Moderate		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	Ports are not listed in the lag creation drop down		
Condition:	When ports are used part of ingress-group or egress (VLAN/TVF), those ports are not listed in drop down during lag creation		
Workaround:	Remove the ports from ingress group or egress before creating the lag		
Recovery:	None		

Parent Defect ID:	XVM-2979	Issue ID:	XVM-2979
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	Configuration migration from MLXe to 9920 fails with error message "Region Service Message Processing Timedout"		

Parent Defect ID:	XVM-2979	Issue ID:	XVM-2979
Condition:	This can happen due to network connectivity issues or latency between XVM and target device.		
Workaround:	Retry export configuration operation.		

Parent Defect ID:	XVM-2985	Issue ID:	XVM-2985
Severity:	S3 - Moderate		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	Policy creation for MLXe devices from library has unsupported packet slicing options available.		
Condition:	When policy is created from library page for MLXe devices, packet slicing option is shown to be configured		
Workaround:	Ignore the packet slicing field when creating policy for MLXe devices from library page		
Recovery:	None		

Parent Defect ID:	XVM-2986	Issue ID:	XVM-2986
Severity:	S3 - Moderate		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	UDA Profile import from PCS library to device fails		
Condition:	During the import of UDA profile created on PCS library, failure message is shown in the notification window.		
Workaround:	Create the UDA library directly on the device configuration page and associate it with the ingress-group.		
Recovery:	None		

Parent Defect ID:	XVM-2987	Issue ID:	XVM-2987
Severity:	S3 - Moderate		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	On MLXe device, policy applied on port-channel member port is not updated/ removed when member port is removed from port-channel.		
Condition:	When a member port of the port-channel is removed directly and port-channel is used in ingress-group		
Workaround:	Remove port-channel from ingress-group before changing member ports of the port-channel and add it back to ingress-group.		

Parent Defect ID:	XVM-2998	Issue ID:	XVM-2998
	S2 - Major		

Parent Defect ID:	XVM-2998	Issue ID:	XVM-2998
Severity:			
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	Policy/Route-map are removed from interface		
Condition:	When policy/route-map rule reconciled doesn't have the egress-group is associated with the egress-group		
Workaround:	Remove the ingress-group which is associated with the policy/route-map, update the policy/route-map rules with egress-group and then add the ingress-group with policy/route-map		
Recovery:	Refresh the configuration, then update the ingress-group with policy/route-map		

Parent Defect ID:	XVM-2999	Issue ID:	XVM-2999
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.0
Symptom:	Policy/Route-maps associated with the interfaces are removed		
Condition:	When a rule is added to reconciled route-map.		
Workaround:	Remove ingress group which is associated with the policy/route-map, add the rule to policy/route-map and then add the ingress-group with policy/route-map		
Recovery:	Refresh the configuration and then associate the policy/route-map with ingress-group.		

Parent Defect ID:	XVM-3020	Issue ID:	XVM-3020
Severity:	S3 - Moderate		
Product:	XVM	Reported in Release:	XVM 6.1.1
Symptom:	1. Mismatch seen between the ingress policy dashboard and the device CLI response for the ACLs mapped to an interface. 2. Statistics for an ACL type are missing on the Ingress policy dashboard.		
Condition:	1. Mismatch is seen on ingress policy stats on devices that have scaled configuration. 2. ACL stats will be missing on the dashboard when the CLI is failed due to device connectivity issues.		
Workaround:	Wait for the next statistics data collection that runs on every three minutes.		

Parent Defect ID:	XVM-3027	Issue ID:	XVM-3027
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.1
Symptom:	Removal of port from ingress group is not update on XVM		

Parent Defect ID:	XVM-3027	Issue ID:	XVM-3027
Condition:	When policy is bound with ingress group and port is removed from the ingress group, same is reflected on the device but not on XVM		
Recovery:	Refresh the XVM page or refresh the device configuration		

Parent Defect ID:	XVM-3028	Issue ID:	XVM-3028
Severity:	S3 - Moderate		
Product:	XVM	Reported in Release:	XVM 6.1.1
Symptom:	Description of ports is not reconciled for MLX and SLX devices.		
Condition:	Description of the port is not reconciled for the SLX devices. On MLX devices, the description having underscore " _" is not reconciled.		
Workaround:	For the MLX device, remove the special characters from the description on the device and reconcile the configuration.		

Parent Defect ID:	XVM-3035	Issue ID:	XVM-3035
Severity:	S3 - Moderate		
Product:	XVM	Reported in Release:	XVM 6.1.2
Symptom:	Wrong target firmware version displayed.		
Condition:	During the firmware upgrade in progress, wrong target firmware version is displayed (displays the last directory name).		
Workaround:	Check the firmware version once the firmware upgrade is completed.		

Parent Defect ID:	XVM-3038	Issue ID:	XVM-3038
Severity:	S2 - Major		
Product:	XVM	Reported in Release:	XVM 6.1.2
Condition:	Sometimes, the device config entries can be hidden by the notification icon that appears at the bottom right corner of the application and might hinder the user to interact with the configuration entries		
Workaround:	Refresh the full page to get rid of the notification icon		

Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.