Known Issues

The following tables address known issues open at the time of publication of these release notes. For an updated list of known issues, run the provided query in the Bug Search Tool.

Known Issues in Version 6.2.0.3

The following table addresses open caveats at the time of publication of these release notes. If you have a Cisco support contract, use the following dynamic queries for an updated list of open caveats, run the provided query in the Bug Search Tool:

- Open Firepower Management Center caveats in Version 6.2.0.3
- Open Firepower Management Center Virtual caveats in Version 6.2.0.3
- Open ASA FirePOWER Module caveats in ASA Version 9.7.x

Caveat ID Number	Description
CSCve34221	Internal server error seen on the UI when we enable CC mode
CSCve70800	Prebuilt reports fail to generate immediately due to DiskManager handling of drains
CSCvf27180	Time to upgrade from 6.2.0.3-362 to 6.2.2-1310 takes too long -- 3hr 27mins.
CSCvf61706	White-List page throws error when automatically populated from **Analysis** > **Hosts** events page

Known Issues in Version 6.2.0.2

The following table addresses open caveats at the time of publication of these release notes. If you have a Cisco support contract, use the following dynamic queries for an updated list of open caveats, run the provided query in the Bug Search Tool:

- Open Firepower Management Center caveats in Version 6.2.0.2
- Open Firepower Management Center Virtual caveats in Version 6.2.0.2
- Open ASA FirePOWER Module caveats in ASA Version 9.7.1.x

Caveat ID Number	Description
CSCvd78319	User groups are not available in access control rule after switching to ASDM management
CSCve45573	Internal error message while loading access control policy in Japanese environment
CSCve49858	AMP file detection on windows SMB shares fails after drive is mapped for 30 minutes or more.
CSCve29893	ASA to Threat Defense 6.1.0.2 Migration tool introduces special character "#" to migrate rules
CSCve54036	Mis-match between actual device version and Management Center stored version causes deploy failures
CSCvc24310	Correlation events showing up with random SI Category
CSCve02220	estreamer certificate generates errors with a McAfee ESM generationQualifier verification failed
CSCve53812	SFDataCorrelator still in local management mode after deployed from Management Center
CSCvd63482	SSL Policy goes out of date after Firepower Threat Defense failover
CSCve46186	Snort memcals for startup memory incorrect on Firepower Threat Defense
CSCve45238	Smart Licensing registration fails even after importing CA Cert into Trusted CA Objects
CSCve54719	Policy deployment failure when PF setting contains Security Zone associated with multiple interface
CSCve49778	Threat Defense ICMP platform settings security zones with multiple interfaces not handled properly
CSCvd29934	synchronization and dhcpd daemon exited 100 time(s) while Registering

Caveat ID Number	Description
CSCvc46599	Error message "Unable to translate SSL cipher suite 65535" needs cleaning up
CSCvd74319	Manager gets deleted after upgrade on Firepower 9300 - 6.2.0.1-41
CSCvd58745	ADI process exits one time while registering Firepower Threat Defense device routed/transparent mode
CSCvc16688	Domain join with subdomain with broader object schema fails
CSCve46036	SFDataCorrelator segfault due to null field in internally generated logoff event
CSCvc22001	Should not allow configuration of multiple realms pointing to the same domain.
CSCve55696	UIMP continues to attempt import for deleted users
CSCve45994	User session propagation in Management Center stalls if bookmark is set to the future then corrected
CSCvb63380	Deleting a user from the Firepower Management Center does not function

Known Issues in Version 6.2.0.1

The following table addresses open caveats at the time of publication of these release notes. If you have a Cisco support contract, use the following dynamic queries for an updated list of open caveats, run the provided query in the Bug Search Tool:

- Open Firepower Management Center caveats in Version 6.2.0.1
- Open Firepower Management Center Virtual caveats in Version 6.2.0.1
- Open ASA FirePOWER Module caveats in ASA Version 9.7.1.x

Caveat ID Number	Description
CSCvd78319	User groups are not available in AC rule after Offbox to Onbox switch
CSCvd63482	SSL Policy goes out of date after FTD failover
CSCvc11489	NGFW NAT policy apply failure after editing IPv6 network object
CSCvd29934	synchronization and dhcpd daemon exited 100 time(s) while Registering a FTD to FMC
CSCvd92322	ICMP Any in dst/src ports are saved incorrectly, which can result in broken pre-filter policy

Caveat ID Number	Description
CSCvd71863	After a patch upgrade from 6.2.0-362, software version is not being updated in DatabaseInfo
CSCvd74319	Manager gets deleted after upgrade on SSP3RU - 6.2.0.1-41
CSCvd58745	ADI process exited one time while registering FTD routed or transparent mode to 6.2.0.1-36 FMC
CSCvc16688	Domain join with subdomain with broader object schema fails
CSCvc22001	Should not allow configuration of multiple realms pointing to the same domain.
CSCvc24051	When user cannot be identified change user display from 'Unknown' to something more intuitive
CSCvb63380	Deleting a user from the FMC does not function

Known Issues in Version 6.2.0

Caveat ID Number	Description
CSCun43602	The configured IPv6 address for an ASA FirePOWER module does not display when you run the **show module 1 details** CLI command.
CSCuw79243	If you deploy an intrusion policy to a clustered or stacked 7000 and 8000 Series devices (in Version 6.0.0 known as a high availability pair), Firepower incorrectly counts all devices in the cluster or stack rather than indicating one device for the cluster or stack.
CSCuv86562	Traceback: ASA crash in thread name fover_health_monitoring_thread.
CSCuy65203	If you deploy an intrusion policy with **Drop when Inline** enabled, intrusion events that use the **detection_filter** keyword and are set to drop and generate now display **Dropped** instead of **Would be dropped**.
CSCux67809	Executing the **show crypto key mypubkey rsa** CLI command on an ASA FirePOWER running Firepower Threat Defense erroneously generates device output.
CSCux64898	In some cases, if you deploy an access control policy with the default action set to **Block** and execute the **configure network management-interface disable-event-channel** CLI command, Firepower continues to generate intrusion and connection events when it should not.
CSCux65770	In some cases, if you attempt to log into Firepower with the incorrect password, Firepower incorrectly locks you out of Firepower after two attempts instead of three attempts.

Caveat ID Number	Description
CSCuz17020	Snort is not able to decode traffic.
CSCuz70987	run_qemu_kvm.sh core dumped on 5506 when device low on memory.
CSCuz81740	The Firepower Threat Defense device overwrites core files configuration of FXOS when it should not.
CSCva40041	If you enable failopen on a series 3 device configured with inline sets and then update the device, the device may incorrectly drop link connectivity for up to 10 seconds before it goes into hardware bypass mode.
CSCva40867	If you switch an ASA FirePOWER module from being managed by ASDM to being managed by an Firepower Management Center and the initial device registration fails, but the device eventually successfully registers to the Firepower Management Center, the network map does not update the status of the device after the failed registration attempt and the Firepower Management Center does not generate an connection events or file events for the device when it should.
CSCva54597	Firepower does not deploy the correct **Regular Expression Limits** default values within the access control policy when you deploy configuration.
CSCva74166	The **show environment** CLI command does not work on Firepower Threat Defense devices.
CSCvb11320	If you edit latency-based performance setting values on the Advanced tab of the access control policy editor page and deploy to a registered Firepower Threat Defense device, Firepower does not save the correct latency rule values when it should.
CSCvb39435	If you deploy a file policy to a device with an excessive amount of endpoints configured, Firepower may experience high CPU use and network latency. As a workaround, redeploy configuration.
CSCvb46169	GRE tunnel flow matches QoS rule ID 0.
CSCvb61021	The **show ipv6 ospf neighbor** CLI command does not work on Firepower Threat Defense devices. As a workaround, execute the **system support diagnostic-cli** CLI command and then execute the **show ipv6 ospf neighbor** CLI command again.
CSCvb61805	Firepower Device Manager 5506 deployment takes about a minute more in Version 6.2.0.
CSCvb62117	You cannot change the master role, remove a unit, or execute on a selected unit from a clustered Firepower Threat Defense device via the following CLI commands: **cluster primary security module**, **cluster exec unit**, and cluster remove unit. To use these commands, you must include the unit number as seen from the output of the show cluster info CLI command: **cluster master unit unit-1-1**.

Caveat ID Number	Description
CSCvb62508	Missing suboptions under capture command from converged cli to capture only blacklisted blocked packets.
CSCvb75308	Rate Limiting **may not** take effect on trusted FTP/TFTP data channel in a cluster deployment.
CSCvb77003	Firepower Device Manager- Unable to filter connection events using zones.
CSCvb79547	If you are using ASDM to manage an ASA FirePOWER module, access control policy comparison does not work. This means you cannot display the differences between your running configuration and your planned changes.
CSCvb80626	In rare cases, Firepower Threat Defense Virtual with low memory allocation does not detect some of intrusion policy violations.
CSCvb88724	The **clear conn** CLI command on the Firepower Threat Defense device only allows you to enter a single IP address for the source or destination; any connections matching the IP address for either the source OR destination are cleared. The CLI help shows that you can enter both a source and destination IP address, but you can only enter 1 address.
CSCvb92548	ASA matches incorrect ACL with object-group-search enabled.
CSCvc01792	Some Firepower Threat Defense commands are model-specific, but may be visible on non-supported models. If you enter an unsupported command, you see the following error: **-ERROR: % Invalid input detected at '^' marker**. Check your command in the Firepower Threat Defense Command Reference Guide for model limitations.
CSCvc03720	The **clear mac-address-table** CLI command is only supported on devices deployed in transparent mode when it should be supported on devices deployed in transparent and routed mode. As a workaround, execute the **system support diagnostic-cli** CLI command for devices deployed in routed mode.
CSCvc05098	If the active Firepower Management Center of a high availability pair fails and the standby Firepower Management Center continues to process traffic while the pair is in a degraded state, then the active Firepower Management Center recovers, Firepower incorrectly displays unknown user for events generated during the degraded state for up to 24 hours before correcting.
CSCvc09167	Firewall rules may not be in sync with firmware rules following policy apply.
CSCvc26721	Management interface receives no traffic after port flap or failover on 5506/5508/5516.
CSCvc35890	If you deploy configuration, Firepower may experience a prolonged amount of time writing syslogs and incorrectly trigger Automatic Application Bypass (AAB) when it should not.
CSCvc38425	ASA with FirePOWER module generates traceback and reloads.

Caveat ID Number	Description
CSCvc41387	If you click the help icon next to the filter textbox, Firepower incorrectly generates an **Error 404: Page not found** error. As a workaround, search the Online Help **Help** > **Online** for intrusion policy keywords.
CSCvc46502	If intra-clustered Firepower Threat Defense devices configured with passive mode or inline tap interfaces experience fragmented traffic, virtual reassembly may fail and the device incorrectly drops traffic. As a workaround, restart the device.
CSCvc50022	Firepower may not be able to process as many HTTP connections in Version 6.2.0 compared to Version 6.1.0.
CSCvc51442	Firepower Threat Defense virtual: ESXi standalone having trouble with serial number.
CSCvc51459	If you run the **managed_pruning.pl** CLI command on an Firepower Management Center and click **Purge Event database & (2)**, the script generates an extraneous warning after purging the database.
CSCvc52879	Reloading Active unit in Active/Standby ASA failover pair is not triggering a failover.
CSCvc53140	OSPF retransmissions and VPN tunnels lost after Active ASA reload.
CSCvc53558	If you add a 10GB management interface to a Firepower Management Center, adding fails and Firepower generates an **unable to change mode for eth2** error.
CSCvc54069	If you create a VPN connection with a reverse route that is same as the already present static route on a Firepower Threat Defense device, then restart the device, the static route breaks and you cannot successfully use the VPN connection.
CSCvc55105	The web interface pages of a Firepower Management Center running Version 6.2.0 takes longer to load than the pages of a Firepower Management Center running Version 6.1.0.x
CSCvc55674	A resource depletion issue can occur on the ASA 5516-X if more than 500 concurrent IPsec or SSL connections are established to the unit. This is unrelated to the maximum IPsec/IKE endpoint count and pertains only to IPsec (either ESP or NAT-T) or SSL connections. The resource depletion will trigger an error and prevent new IPsec or SSL connections from being created to the unit. This issue is specific to the ASA 5506/5508/5516-X family of devices, but is most likely to be seen with the ASA 5516-X. No other ASA FirePOWER modules are affected by this issue.
CSCvc56526	CEP records edit page take minutes to load.
CSCvc56717	In some cases, if Firepower experiences a database error and you attempt to create a domain, you may not be able to delete a domain or move a device to a domain.
CSCvc56746	The Objects page in the FC2000 and FC4000 web interface takes more time to load in Version 6.2 compared to Version 6.1.x.

Caveat ID Number	Description
CSCvc56767	The FC2000 web interface takes more time to save an access control policy in Version 6.2 compared to Version 6.1.x.
CSCvc56919	Traffic drops for reverse UDP/TCP IPv6 traffic over IPv4 tunnel.
CSCvc58132	When upgrading Firepower Threat Defense, Firepower may fail to detect applications during the upgrade. Issue will be automatically resolved once deployment is manually triggered post upgrade.
CSCvc58296	In some cases, if you update Firepower and configure Open Shortest Path First (OSPF) in the Dynamic Routing tab of the Virtual router page (**Devices > Devices Management > Virtual routers > Dynamic Routing**), Firepower does not display the available routes when it should. As a workaround, restart the managed device. .
CSCvc58453	Firepower Threat Defense devices running FXOS Version 2.1.1(64) do not support Firepower Version 6.1.0.
CSCvc58272	ASA incorrectly processing negative numbers in wrappers, resulting in graphical webvpn issue.
CSCvc58398	Firepower Management Center warnings needed during high availability configuration that configuration on standby will be wiped.
CSCvc59613	If you assign both an active and standby MAC address to a registered Firepower 4100 series or Firepower 9300 high availability pair with the **Add Interface MAC Address** option in the High Availability tab of the Integration page **System** > **Integration** and deploy, then edit the interfaces and delete the interface, Firepower does not delete the MAC address associated with the interface after synchronizing the pair and redeploying fails. As a workaround, delete both the interface and the MAC address associated with the interface, then synchronize changes and redeploy.
CSCvc59811	If you place an access control rule configured to **Allow** a subdomain URL (site.example.com) above an access control rule configured to **Block** the domain URL (example.com), the system may block request to subdomain URL. As a workaround, create an access control to **Allow** each subdomain URL (site.example.com, site2.example.com, etc.) you do not want blocked instead of the rule to block the domain URL, then save and redeploy.
CSCvc60254	SIP: 200 OK messages with multiple seqments not reassembled correctly.
CSCvc62252	Tracking route is up while the reachability is down.
CSCvc62492	ASA: File system becomes read-only after very long up time.
CSCvc62556	Traceback in ASA Cluster Thread Name: qos_metric_daemon.
CSCvc63722	Report Generation of large no of Events is failing.

Caveat ID Number	Description
CSCvc63954	ASA traceback in Thread Name: Event mib process.
CSCvc64050	ASAConfig uses wrong interface IDs after slave unit rejoins multi context ASA cluster.
CSCvc65262	After Snort restart, UDP processing performance may decrease.
CSCvc65409	Traceback observed on gtpv2_process_msg on cluster.
CSCvc65470	In some cases, connection events and security intelligence events generated from identity policy activity show the **Initiator User 0** instead of the username.
CSCvc65528	Pages in the MC4000 web interface take more time to load in Version 6.2.0 compared to Version 6.1.x.
CSCvc68358	The **show lacp** CLI command does not work on ASA 5585-X devices.
CSCvc74395	If you deploy an access control policy containing an access rule with Original Client IP, logging enabled and an SSL rule with the default actions set to **Decrypt - Resign**, Firepower does not display the Action and Access control rule columns of some generated events in the Connection Events page **Analysis** > **Connections** > **Connection Events**.
CSCvc75561	If you use non-ASCII characters in a Flex Config object, the Flex Config policy fails to deploy. As a workaround, replace the non-ASCII characters with the ASCII equivalents.
CSCvc76439	If you create a GID:135 intrusion rule, the rule does not save and Firepower generates a **failed to set the rule state** error.
CSCvc79719	SMB upload - Malware block miss on first attempt.
CSCvc81525	In rare cases, Firepower Threat Defense devices managed by the Firepower Device Manager and ASA with FirePOWER Services devices managed with ASDM can experience an exhaustion of database handles, which prevents any attempt to upgrade to Version 6.2.0. Prior to running the upgrade, contact Cisco TAC to enable upgrade by restarting the appropriate processes.
CSCvc82066	If you update a Firepower Management Center from Version 6.1.0 to 6.2.0 and deploy, deployment may fail and Firepower may generate a **mtu 9188 ^ ERROR: % Invalid input detected at '^' marker.** error message. As a workaround, change the MTU value before you update to Version 6.2.0.
CSCvc92934	If you deploy an access control policy containing an access control rule configured to **Allow** a subdomain URL (site.example.com) placed before an access control rule configured to **Block** the domain URL (example.com) that references an SSL policy with decryption enabled, the system may inconsistently match traffic against the HTTPs certificate instead of the actual URL and navigating to the subdomain may get blocked when it should not.