Illumio® Core
Version: 21.1.0

Release Notes

03/16/2021

14000-100-21.1.0

illumio

Contents

Welcome

These release notes describe the resolved issues and known issues for the Illumio Core 21.1.0 release.

Document Last Revised: March 2021
Document ID: 14000-100-21.1.0

> ⚠ The Illumio Core platform was previously known as the Illumio Adaptive Security Platform (ASP). References to "Adaptive Security Platform" and ASP still appear in these release notes.

What's New in This Release

To learn what's new and changed in 21.1.0, see What's New in This Release on the Illumio Technical Information portal.

Security Information

For information about security issues, security advisories, and other security guidance pertaining to this release, see Illumio's Knowledge Base in Illumio's Support portal.

Product Version

Current PCE Version: 21.1.0+H1
Current VEN Version: 21.1.0+H1

Release Types and Numbering

Illumio ASP release numbering uses the following format: "a.b.c-d+e"

- "a.b": Standard or LTS release number, for example, "21.1"
- ".c": Maintenance release number, for example, ".1"
- "-d": Optional descriptor for pre-release versions, for example, "preview2"
- "+e": Hot Fix release descriptor, for example, "+H1", "+H2", "+H3".

Resolved Issues in 21.1.0+H1-PCE

- **PCE performance for customers could be slow** (E-76377)
  When backing up the PCE database, Illumio customers could experience slow performance during Explorer queries, especially when the traffic database was reaching disk limits. This issue is resolved. Customers will no longer potentially experience slow performance with Explorer queries during their database maintenance for the PCE.
- **Occasional issues with rules** (E-76344)
  In rare circumstances, some issues with rules were seen, where the VEN used to enforce incorrect IP addresses in the policy. This may have been caused by workloads (instead of labels) being used extensively in rules. Issues of this nature have been resolved.
- **User interface issues have been resolved** (E-76614)
  The user interface intermittently used to display the list of Virtual Servers as "Unassociated" instead of the expected Management State. This issue has been resolved.

Resolved Issue in 21.1.0+H1-VEN

- **VENs running on Windows hosts experienced high memory usage** (E-76748)
  On managed Windows workloads, a Windows firewall process consumed excessive kernel memory over time. This issue occurred when the environment managed by the PCE experienced high policy churn. Unchecked, the process could cause the Windows system to crash. This issue is resolved. On managed Windows workloads, the firewall process that was causing this issue no longer consumes excessive memory even in a high policy churn environment.

Resolved Issues in 21.1.0

PCE Web Console

- **Events filtering result wasn't correct** (E-72755)
  Filtering events by the failure status could also return events that had a successful status. This issue is resolved. In this release, the PCE web console can correctly filters events to display only events that have the failure status.

Policy and Workloads

- **Workload list page did not load and timed out** (E-75575)
  Upon requesting to display the Workloads list page in the UI, the page failed to load, and a

TimeoutError message was displayed. The issue occurred only when the Vulnerability Map was enabled. This issue has been resolved.

- **An offline workload should have generated an event** (E-73778)
  A workload that was marked “offline” by the Decommission and IP Cleanup Timer, should have generated an event when the workload was actually removed from the policy. However, it did not. This issue has been resolved.

Data Visualization

- **Dropped packet and traffic flows error 500 failures** (E-75451)
  In a supercluster, one of the core nodes was reporting error 500 failures for traffic flows and dropped packet requests.
  This issue has been resolved.
- **Unable to import big vulnerability reports due to requests timing out** (E-75124)
  Users were unable to import a vulnerability report when it contained more than 100K vulnerability entries and It was getting timed out errors on the client side.
  This issue has been resolved.
- **Issues with "Deep Analysis Rule" in the Explorer's draft view** (E-75016)
  In the Explorer's draft view, "Deep Analysis Rule" was showing flows as blocked while "Quick response" was showing them as allowed. Deep Rule Analysis was not handling Container Workloads correctly, so it only worked for workloads.
- **Scaledata selection throws a console error** (E-74803)
  The Policy Generator was failing for highly connected App Groups and a console error was thrown.
  This issue has been resolved.
- **Problem with flow endpoint mapping to an Unmanaged workload** (E-74773)
  Users reported a problem in Explorer with flow endpoints not being mapped to specific unmanaged workload even though the IP shown in flow record belongs to that workload. This issue has been resolved and Explorer now displays the correct flow endpoint mapping to the workload.
- **Explorer times out on traffic queries** (E-74160)
  There were performance issues with the Explorer queries on large sets of data. This issue was resolved by adding indices on older tables, which should improve the query performance.
- **Explorer Draft View - IP lists with exclusions** (E-74118)
  In the Explorer Draft View, traffic might have been incorrectly shown as allowed to an IP list with 0.0.0.0/0 and exclusions, when the traffic matches the excluded IP(s).
  This issue has been resolved.
- **Traffic not properly updated in Illumination** (E-73998)
  Traffic Flow link was not changing to blocked traffic from potentially blocked traffic.
  This issue has been resolved.

- **Selecting Explorer from App Group failed when AppGroup mode was set to APP-ENV-LOC instead of APP-ENV** (E-73815)
  When you right-clicked and selected Explorer from Illumination, and the App-Group mode was set to APP-ENV instead of APP-ENV-LOC, you were not able to select the GO button. This issue has been resolved.
- **Incremental upload of vulnerabilities might cause duplicated rows** (E-73500)
  Incremental upload would result in duplicated rows when vulnerability reports with port or proto set to nil were imported twice for the same workload.
  This issue has been resolved.
- **Number of locations in the global Illumination map maxed at 199** (E-71342)
  Number of locations in the Location View was not displaying more than 199 locations as location bubbles.
  This issue has been resolved by adding the following message in the UI: "The number of locations exceeds the maximum that can be displayed in Illumination. Please use the Search bar to select a location for viewing".
- **Illumination map does not draw traffic correctly** (E-72927)
  Illumination map did not draw traffic to virtual services for ipv6 and publicly routable address overrides.
  This issue has been resolved.
- **Illumination and App Group Map issues** (E-72926, E-74425)
  After upgrading the PCE to 20.2, a few parts of the PCE Web Console appeared to be hung up.
  This issue is resolved. The Web Console now works as expected.

PCE Platform

- **Multiple instances of avn_perfmon.sh running** (E-65673)
  The performance monitoring script `avn_perfmon.sh` is scheduled to run at regular intervals. In the presence of stale NFS partitions, this script could get stuck trying to determine the disk usage of the stale partitions. This caused an increasing number of stuck instances of the script over time. This issue has been resolved. The script no longer probes stale partitions, and only one instance can run at the same time.
- **Items didn't match label filters** (E-62880)
  When filtering objects (Workloads, Virtual Services) by label, items were suggested even if they did not match the label filters that had already been selected. This issue has been resolved. Only items that match the label filters are presented.
- **The disk was filled with core files, though this caused no disruption in PCE functionality** (E-74367)
  An internal monitoring process used to trigger a segfault due to a driver incompatibility. This resulted in excessive core files filling up disk space. However, it did not disrupt the PCE from functioning normally. This issue has been resolved.

- **Asynchronous call to app_groups API failed without max_results parameter** (E-74651)
  When the `app_groups` API was called as an asynchronous request, and the `max_results` parame ter was not provided, the call failed. This issue has been resolved.
- **PCE support report omitted systats directory when duration flag was used** (E-74178)
  When the PCE `support_report` command-line tool was run to collect logs and system statistics for a time window specified with the optional flag `duration`, the generated support report did not include the files in the `systats` directory. This issue has been resolved.

Containers

- **Incorrect banner was displayed** (E-71950)
  When logged in to a domain other than the one in which the cluster was created or logged in to a member of a supercluster (not the leader), a banner incorrectly read that a virtual service was owned by another container cluster. This issue did not affect functionality, and it has been resolved. The banner language has been corrected. When the virtual service was created by a container cluster that has been deleted, the banner informs the user of the deletion and describes actions that can be taken.

REST API

- **Clearing traffic returned 500 error** (E-75377)
  This error occurred when Illumination backed by the traffic database was enabled. The network traffic API returned 500 API errors when traffic was cleared. This was caused by a missing method. This issue has been resolved.

VEN

- **The VEN dropped Broadcast traffic** (E-75811)
  When the VEN was in enforced mode, all broadcast traffic was dropped because of a rule that was mistakenly placed at the start of the firewall policy instead of after the allowlist policy. The goal of the "drop all" broadcasts policy was to reduce the number of dropped broadcast packets being passed on to the PCE. This issue has been resolved.
- **VEN tampering detection occurs due to nft incompatibility in RedHat 8.3** (E-75399)
  On a device running Red Hat 8.3, VEN tampering was detected every 10 minutes. This issue has been resolved.
- **VENs running in an AWS environment reported "agent.tampering" messages** (E-74449)
  VENs running certain versions of Linux in AWS used to display “agent.tampering” messages. This issue has been resolved.

- **Linux VEN on a DNS server consumed high memory and CPU cycles** (E-74446)
  A Linux VEN running on a DNS server was memory intensive and consumed high CPU cycles. This issue has been resolved.
- **AUS did not work with default AD group "Domain Users"** (E-73769)
  When the Adaptive User Segmentation (AUS) rule, that uses the "Domain Users" Active Directory user group was skipped, it caused traffic to be blocked. This issue has been resolved.
- **All KB articles did not get downloaded on a Windows VEN** (E-73725)
  When a support report was being generated, the VEN did not list all the knowledge base (KB) articles currently installed in the OS. This issue has been resolved. A complete list of KB articles is now gathered into a new file called "hotfixes" under the system directory of the report.
- **High CPU consumption issue resolved** (E-74538)
  Under some circumstances, the Windows Performance Monitor reported the VEN Platform Handler service's high levels of CPU consumption. Typically, this occurred when the FQDN cache manager performed FQDN cache maintenance. This issue has been resolved.
- **Some audit messages no longer appear in Windows 8** (E-73780)
  In Windows 8 or later, the VEN will no longer enable audit for the following messages:
  MPSSVC Rule-Level Policy Change
  IPsec Main Mode
  IPsec Quick Mode
- **Windows VEN wasn't displaying system events** (E-72860)
  On Windows workloads, the Windows Event Viewer wasn't displaying system events when VEN processes started or stopped, or when configuration updates occurred. This issue has been resolved. In this release, the Windows Event Viewer correctly displays system events for VEN processes.
- **DNS Server Policy Application Performance** (E-75867, E-61926)
  On a DNS server (such as, Windows AD/DNS or Linux BIND server), prior to Release 21.1.0, the VEN did not distinguish between requests from applications running on the server or requests that the server sent on behalf of client machines to resolve out-of-zone requests. This was especially true for DNS servers that were running in recursive mode. As a result, on DNS servers, the VEN intercepted a large number of responses that were forwarded back to the clients. Since all DNS responses were intercepted, processed, and stored in the VEN's database on the server, it impacted the policy application performance. From Release 21.1.0 onwards, the VEN will only intercept DNS response for requests sent by applications that run on the DNS server itself. As a result, the policy application performance will improve.
- **Packet Filter issues were seen on Solaris 11.4 during policy changes** (E-69769)
  On Solaris 11.4, the VEN firewall process would configure the PF tables (accidentally flushing the firewall rules) and then would configure the PF firewall rules. During this process, there was a minuscule window (typically a fraction of a second) when no firewall policy was in effect. This issue has been resolved.

- **Degraded infrastructure on VENs consume high CPU** (E-75087)
  When a Linux VM was paired with a VEN in degraded mode, and the VM had a high volume of traffic, it caused high CPU and disk I/O operations. This issue has been resolved.

Known Issues in 21.1.0

REST API

- **Exposure roll back for sec_policy_get.schema.json** (E-76331)
  In this release, the `sec_policy` schemas are explicitly indicating that the `selective_enforcement_rules` are Public Experimental. This explicit clarification indicates that the `selective_enforcement_rules` objects may change in the future.

PCE Web Console

- **Online help sometimes does not display information in the help pop up** (E-75943)
  The Help pop up sometimes does not display information when it launches a separate pop up window. For example, when you click on the question mark icon and the Help pop out appears, if you click the upward arrow, the new window that is launched contains no information.
- **Specifying multiple labels within each label type is not supported** (E-73039)
  You can filter one label per Role, Application, Environment, or Location label type. While you have the ability to indicate multiple labels in your search filter within each type, you will not receive any results.
- **Incorrect count in selector static categories** (E-68895)
  When a user enters a value in a selector in the PCE web console, the options matching the input are displayed along with the matched and total count. In the case of Static categories, the matched count is correct but the total count displayed is incorrect.
  Workaround: While a workaround is not available, the issue occurs only when the user filters a static category. The matched count is correct but the total count is incorrect and will be fixed in a future release.
- **No error message is displayed after typing in an invalid port** (E-68255)
  When you enter an invalid port number while editing a service, the PCE still displays options to select from. When you move to another field without making a selection, the entered letters/digits are not cleared to reflect that the entered value was not selected. It can appear that the value you entered was accepted even though invalid.
  Workaround: Press ENTER after entering text. When the combination was valid, it will be selected. Otherwise, it will be cleared.

- **Filtering by an Invalid Protocol in the Services List page displays all services** (E-68251)
  When you type an invalid protocol and presses ENTER, the protocol appears as a filter item but the list page is not refreshed. The PCE web console validates the entered protocol and refreshes the page only when the protocol is valid.
  Workaround: There is no workaround but this is only a cosmetic issue.
- **Filtering by an invalid port in the Services List page displays an error** (E-68249)
  When you filter the Services list using an invalid port, you receive the 406 error: "Port value out of range." The port filter category is a free search and your input is passed to the PCE without validation.
  Workaround: Clear the entered port number and filter the list with a value in the valid port range.
- **The wildcard in workloads filter not working** (E-65232)
  In the Workloads page of the PCE web console, the filter field should accept the asterisk (*) wildcard in filter expressions to filter the workload list; see Use a Wildcard to Filter Workloads. However, while the PCE web console accepts the asterisk as a valid character, the filter will always return zero results, even when there are workloads that should match the filter expression.
- **Filter doesn't handle the percentage symbol** (E-64904)
  When users select a filter option from the drop-down list, the selected value is added to the URL. When the selected value contains the percentage symbol (%), the PCE web console displays an error and a blank page appears.
  There is no workaround; however, this is a rare situation because the % symbol is not used often in values.
- **Pressing Enter doesn't select the default option in the dialog box** (E-53831)
  When the PCE web console displays a dialog box, pressing **Enter** might select an action other than the default.
  Workaround: Use your mouse to click the required button in the dialog.

Policy and Workloads

- **Virtual Servers rules tab does not display IP addresses of pods** (E-74635)
  The IP addresses on the rules tab of a Virtual Server displays only host IP addresses and not the container workload IP addresses.
- **Incorrect error message displayed when rule set renamed to a name that's in use** (E-74498)
  On creating and provisioning rule set, for example rule set A, renaming it to B, then creating rule set A and reverting modifications to rule set B, the UI displays an incorrect ‘500’ error instead of an error message informing that the rule set name is already in use.
- **Policy restore impacts the virtual services of a container cluster** (E-73979)
  The existing issues are as follows:

    - When policy is restored to a version before the creation of a container cluster's virtual services, the container cluster's virtual services are marked for deletion in the draft change.
    - When a container cluster is deleted, restoring its virtual services is possible through policy restore.
- **Rule search incorrectly calculates label-groups in Scopes** (E-72318)
  When a rule has label groups in the scope, multiple scopes are created and traffic is not allowed between scopes unless specified with extra-scope rules. For example, Workload 1 and Workload 2 cannot talk to each other based on the policy because they are in different scopes. However, rule search for Workload 1 to Workload 2 allows access by this rule.
- **Inconsistencies in rule coverage for the Windows process-based rules** (E-71700)
  The draft view of Illumination and Explorer may show an incorrect draft policy decision for traffic covered by a rule using a service with a Windows process or service name. This generally happens when there is a port/protocol specified in the rule in addition to the process/service name, or when a non-TCP/UDP protocol is used in the rule. In these cases, the reported view will provide the correct policy decision as reported by the VEN based on the active policy.
- **'Upgrade' option is enabled for a Read-Only User in VENs list** (E-70341)
  After logging in as a Read-Only user, on navigating to the VENs list page, the 'Upgrade' option is enabled instead of being disabled.
- **The timestamp "updated_at" not changed when a workload label is edited** (E-68720)
  When workload labels are updated through the API or the PCE web console, the timestamp "updated_at" in the workload API response will not be updated. This field is not visible in the PCE web console.
  There is no workaround. The issue affects only the timestamp and no other PCE functionality.
- **Incorrect Group Label count is displayed while editing a group for a workload** (E-68691)
  Workaround: This issue can be resolved by backend providing a subset of results with the total filtered count.
- **Rule search with virtual service and labels returns an incorrect rule** (E-65081)
  When a rule is written with a virtual service whose labels conflict with the ruleset scope, and a rule search is done for the virtual service, the rule search may return the rule even though the rule does not apply due to the scope conflict.
  Workaround: Use the rule search to ensure that the rule applies to the virtual services and the scope labels separately.
- **Label groups aren't allowed for scoped user when adding/updating rule set but choice appears in UI** (E-63960)
  In the PCE Web Console's Add Ruleset dialog, when a user with a scoped role chooses a label group in one of the Scope fields, the message "You cannot modify Rulesets with broader Scope(s) than your permitted Scope(s)" is displayed. The error is caused by the UI improperly presenting a scoped user with the choice to select a label group. The choice should not have appeared in the drop-down list. (For more information about scoped user roles, see About

Roles, Scopes, and Granted Access in the PCE Administration Guide.)
Workaround: When logged in as a scoped user, do not select label groups in the Scope fields when adding or modifying a rule set.

- **Incorrect user name in Support Reports page after generating report from VEN** (E-62935)
  After generating a support report from VEN using the `illumio-pce-ctl` command, the Support Reports page on the PCE displays either an incorrect user name or "Unknown" for the generated support report.
- **Clicking deleted ruleset in Policy Versions shows "Resource Not Found"** (E-62929)
  In the PCE web console **Policy Versions** page, when you click the name of a deleted ruleset, the message "Resource Not Found" is displayed. This is because the deleted ruleset does not exist in that version. The message is correct but not as informative as it could be.
- **Cannot create a rule with a label type defined in the Scope** (E-59100)
  In the PCE web console, you cannot create a rule with a label type that has also been used in the scope.
  Workaround: You can create such a rule using the API.
- **Unable to select multiple protocols in Rule Search** (E-57782)
  When you try to select multiple protocols in Rule Search, you cannot select a second protocol after selecting a protocol once. For example, you select TCP and then want to select UDP, the PCE web console does not display the protocol option again.
  Workaround: Use the REST API to select multiple protocols and obtain the correct search results. The above issue happens only in the PCE web console.

Data Visualization

- **"Visibility Only" Workload Filter does work properly** (E-74231)
  Applying the "Visibility Only" workload filter does not reduce the Connected App Groups count reliably and can be changed again after a refresh.
  Workaround: Not available
- **Vulnerability - V-E score is not showing correctly** (E-73277)
  V-E score is not correct when compared with V-E score column and Total V-E score. For example, when adding V-E score column showing as a 69.8 the Total is showing as 71 instead of 70.
  Workaround: Not available
- **VES and E/W exposures wrong for the internet and other workloads** (E-73023)
  If a rule provides a service on a vulnerable port/protocol to the internet and to some set of workloads, the workloads in the port exposure are not counted. This leads to a VES of 0 instead of larger than 0. The exposure calculation is correct if the internet is not provided as a consumer.
  Workaround: n/a
- **Command panels close on navigating to the map from the details page** (E-71502)
  The workload, container workload, and virtual services command panels close when you

navigate to the map from the details page. This issue is due to redirecting between map page and workload, virtual services, container workload details page, which are built using different modules.
Workaround: Re-select the element on the map to reopen the command panel.

- **Add Rule panel not displaying for selected traffic with right-click actions** (E-68548)
  On right-clicking on selected traffic and clicking Add Rule, the Add Rule panel should display for selected traffic. Instead of the current selection, it displays the previous Add Rule panel for other selected traffic.
- **In Illumination, after dragging unlabeled workload into and joining an App Group, it can move out of the App Group** (E-66659)
  When dragging an unlabeled workload to join an App Group, users might observe the workload moving toward the bubble boundary of the App Group. To have the workload move back inside of its App Group, refresh the browser page or refresh Illumination using the PCE web console. Workaround: None; however, this issue is cosmetic only.

PCE Platform

- **Attempt to create API key on supercluster member returns incorrect error code** (E-75627)
  When an attempt is made to create a new API key with a POST call to the `api_keys` endpoint on a PCE that is a member of a supercluster, the API returns an error. This is the expected behavior, because creating an API key on a supercluster member is not allowed. The API returns a 500 error, which is the incorrect code; it should be 403.
- **agent.activate events not always classified correctly** (E-74682)
  Events generated when an agent is activated (`agent.activate` events) are categorized inconsistently. Success events are classified as auditable, and failure events are categorized as `system_events`.
- **Filter is not applied when downloading events** (E-74450)
  On the Events page, when the Export Filtered button is clicked, the filter is not applied. All the events are downloaded.
- **Health check failed to update status** (E-71526)
  The Node Status field is not always reflected in the PCE Health Summary.
  Workaround: Inspect the individual state under the Node tab to see if there are any issues.
- **PCE sometimes fails to start** (E-73518, E-60012)
  The PCE services may fail to start with one or more nodes stuck in PARTIAL state. When this error occurs, running the command `illumio-pce-ctl status -v -s` on a node in PARTIAL state shows the status of `consul-agent` or `service-discovery` and other services as NOT RUNNING. This may be caused by the service startup scripts failing to completely start the Consul agent or to detect that it has been started successfully before the timeout.
  Workaround: Try starting the PCE services again on nodes where they are in PARTIAL state.

- **Resource change in event type rule_set.update doesn't represent scope of change** (E-52732)
  When a rule set is changed, the event type `rule_set.update` incorrectly represents the scope of the change as individual scope objects, instead of as an array of those scope objects.
- **PCE uptime value can be wrong in the PCE Health page** (E-45143)
  Temporary, expected PCE service restarts can reset the PCE uptime values displayed in the PCE web console PCE Health page so that it is not consistent with the uptime values displayed by `illumio-pce-ctl start`.

RBAC and Authentication

- **Label groups aren't allowed for scoped user when adding/updating rule set but choice appears in PCE web console** (E-63960)
  In the PCE web console **Add Ruleset** dialog, when a user with a scoped role chooses a label group in one of the Scope fields, the message "You cannot modify Rulesets with broader Scope(s) than your permitted Scope(s)" is displayed. The error is caused by the PCE web console improperly presenting a scoped user with the choice to select a label group. The choice should not have appeared in the drop-down list. (For more information about scoped user roles, see About Roles, Scopes, and Granted Access in the PCE Administration Guide.)
  Workaround: When logged in as a scoped user, do not select label groups in the Scope fields when adding or modifying a rule set.

Containers

- **IKS VPN Pod traffic not showing in Illumination/Explorer** (E-71163)
  You may not see long lived flows that were established before the firewall is programmed for container workloads (this does not apply to host workloads). There is no workaround because it's a feature that has not yet been implemented for container workloads and not an issue.
- **Outbound rule opens up both TCP and UDP ports** (E-60837)
  When a Kubernetes service has both port 1234/TCP and port 2345/UDP configured, a rule configured with the pod as Consumer and Virtual Service as Provider will open up both ports 1234/TCP and 2345/TCP as well as 1234/UDP and 2345/UDP on the pod's firewall (outbound rule). This configuration is supported with Illumio ASP. In this case, only the port number associated to the port statement will show this issue, the port number associated to the targetPort statement will not show this issue and will attach to the protocol specified in the Service YAML file. For more information and an example, see *Illumio ASP for Kubernetes and OpenShift*.

VEN

- **PowerShell failure error messages appear when you try to pair the Windows 7 and Windows Server 2008 R2 VEN** (E-75974)
  On Windows 7 and Windows Server 2008 R2 VENs, though the VEN pairing process is successful, you may see some PowerShell failure errors. You may ignore these messages since the pairing process is successful.

All Platforms: VEN Known Issues

- **platform.log shows "No such file or directory" and "Could not set connect ion policy to loose error" errors** (E-71943)
  Error messages similar to these show up in platform.log:
  ```
  2020-09-29T10:41:36.126-07:00 INFO:: TCP loose connection grace period set to zero. Disabling strict tcp connections.
  2020-09-29T10:41:36.186-07:00 ERROR:: Could not set connection policy to loose error
  ```
  Cause: VEN transitions between managed and unmanaged (Idle) state before conntrack check timer expires. No workaround is required. The VEN will recover itself once it is in a managed state (out of Idle) and the conntrack loose timer expires.
- **VEN generates event with severity Err instead of Info when the unsuspend command is run twice** (E-69196)
  Unsuspend a VEN by using the PCE web console or REST API so that the VEN is active. Then, unsuspend the VEN using the command `/opt/illumio-ven/illumio-vent-ctl unsuspend`. The VEN generates an event with severity Err when it should be severity Info.
- **Upgrading VEN on workload can cause API to generate 406 error** (E-40132)
  This API error occurs when the API version is incompatible with the VEN. Every 24 hours the VEN retrieves a new master configuration file, which will correct the API version incompatibility.
  Workaround: In most cases, this issue corrects itself within a few minutes. When it does not, wait for the VEN to retrieve a new master configuration file or restart the VEN to force it to update the file.

Linux VEN Known Issues

- **Upgrading Linux VEN to 19.3.x and later doesn't load Illumio firewall after VEN starts** (E-71122)
  Upgrading a Linux VEN from ASP 17. *x* or 18. *x* to ASP 19.3. *x* or later releases (such as 20.2.0) can fail to load the Illumio firewall after the host and VEN restart. This issue only occurs on RHEL8/CentOS 8 when the VEN is stopped prior to upgrading to the later ASP release and the host is rebooted before the VEN attempts to retrieve the new nftables-based firewall from

the PCE.
To work around this issue, perform any one of the following actions:

- Do not stop the VEN before upgrading it to the later release, such as 20.2.0.
- When you must stop the VEN before upgrading it to 20.2.0, restart the VEN before rebooting the host.
- Before upgrading the VEN to 20.2.0, ensure that the VEN can connect to the PCE to obtain its Illumio firewall.
- Do not reboot the host until after nftables has loaded the Illumio firewall. Run the `nft list ruleset` command to confirm that the Illumio firewall loaded. Illumio rules should be present.

Solaris VEN Known Issues

- **Repeated logs observed in vtap.log after restarting VEN on Solaris** (E-63072)
  The message `INFO: Waiting for first reconcile file` is logged repeatedly after restarting a VEN. The contents of the Conntrack table are not removed at restart, so long-lived connections established while the VEN was stopped stay active until the next policy change, instead of being marked as "potentially blocked" or removed from the Conntrack table.