



# Cisco Tetration Release Notes

## Release 3.3.2.42

This document describes the features, caveats, and limitations for the Cisco Tetration software, release 3.3.2.42.

The Cisco Tetration platform is designed to comprehensively address a number of data center operational and security challenges using rich traffic telemetry collected from servers, layer 4 through 7 service elements, and end-point devices (such as laptops, desktops, and smartphones). The platform performs advanced analytics using an algorithmic approach to offer a holistic workload protection platform. This algorithmic approach includes unsupervised machine-learning techniques and behavioral analysis. The platform provides a ready-to-use solution supporting the following use cases:

- Provide behavior-based application insight to automate allow-list policy generation
- Provide application segmentation to enable efficient and secure zero-trust implementation
- Provide consistent policy enforcement across on-premises data centers, and private and public clouds
- Identify process behavior deviations, and software vulnerabilities and exposure to reduce attack surface
- Identify application behavior changes and policy compliance deviations in near-real time
- Support comprehensive telemetry processing in a heterogeneous environment to provide actionable insight within minutes
- Enable long-term data retention for deep forensics, analysis, and troubleshooting

To support the analysis and various use cases within the Cisco Tetration platform, consistent telemetry is required from across the data center infrastructure. Rich Cisco Tetration telemetry is collected using agents. There are different types of agents available to support both existing and new data center infrastructures. This release supports the following agent types:

- Software agents installed on virtual machine, bare-metal, or container hosts
- ERSPAN agents that can generate Cisco Tetration telemetry from copied packets
- Telemetry ingestion from ADCs (Application Delivery Controllers) – F5, Citrix and AVI
- NetFlow agents that can generate Cisco Tetration telemetry based on NetFlow v9 or IPFIX records
- Embedded hardware agents in Cisco Nexus 9000 CloudScale series switches

In addition, support is provided for ingesting endpoint device posture, context and telemetry through integrations with

- Cisco AnyConnect, installed on endpoint devices such as laptops, desktops, and smartphones
- Cisco ISE (Identity Services Engine)

Software agents also act as the policy enforcement point for application segmentation. Using this approach, the Cisco Tetration platform enables consistent microsegmentation across public, private, and on-premises deployments. Agents enforce the policy using native operating system capabilities, thereby eliminating the need for the agent to be in the data path, and providing a fail-safe option. **Additional product documentation is listed in the “Related Documentation” section.**

These Release Notes are sometimes updated with new information about restrictions and caveats. See the following website for the most recent version of this document:

<https://www.cisco.com/c/en/us/support/security/tetration/products-release-notes-list.html>

The following table shows the online change history for this document.

Table 1 Online History Change

Date	Description
July 1 <sup>st</sup> , 2020	Release 3.3.2.42 became available.

## Contents

This document includes the following sections:

- [New and Changed Information](#)
- [Caveats](#)
- [Compatibility Information](#)
- [Usage Guidelines](#)
- [Verified Scalability Limits](#)
- [Related Documentation](#)

## New and Changed Information

This section lists the new and changed features in this release and includes the following topics:

- [New Software Features](#)
- [Changes in Behavior](#)
- [Enhancements](#)

### New Software Features

- Software agent support added for Redhat Enterprise Linux 8.1 and SUSE Linux 12 SP5 to support all workload protection capabilities.

### Changes in Behavior

These are changes in behavior for this release:

- Enforcement policies produced for workloads are now bundled. Previously, if a logical policy matched multiple IP addresses belonging to the interfaces of one workload, the logical policy was translated into multiple address-specific concrete policies, one for each IP address. With this patch, only one concrete policy is created for all the matched addresses. This reduces the number of concrete policies for the workload. Furthermore, if a logical policy matches all IP addresses of a workload, the concrete policy will be workload-specific rather than address-specific. This makes it possible to enforce non-disruptive allow-list policies on workloads with DHCP where the IP addresses are subject to change.
- Port generalization in ADM policy generation is performed on outbound policies rather than only on inbound policies, as in previous versions.

## Enhancements

- ADM automatic policy generation performs statistical port generalization for outbound policies to external hosts outside of ADM run scopes.
- AIX software agent improvements
  - Comparative updates to IPPool - minimizing impact to existing sets while enforcing a new policy by the AIX enforcement agent.
  - For AIX 7.1 TL3 SP5 and later, AIX software agent now supports flow capture for up to 16 network interfaces, while leaving four network interfaces as flow capture for the system. For an older AIX version, a maximum of six flow captures are shared between the agent and system.
- When a connector is enabled on a Tetration Ingest appliance, we attempt to clean up any state added by “conntrack” (a utility in Linux to keep track of connection states). This allows the connector (deployed as a container in the appliance) to receive traffic where the source IP of the traffic is preserved. This enhancement requires the use of new OVAs published as part of this release. The new OVAs are optional and are required only if traffic for connectors on the appliances may be set up before the connectors are actually enabled/deployed.

## Caveats

This section contains lists of open and resolved caveats, as well as known behaviors.

- [Open Caveats](#)
- [Resolved Caveats](#)
- [Known Behaviors](#)

## Open Caveats

The following table lists the open caveats in this release. Click a bug ID to access Cisco’s Bug Search Tool to see additional information about that bug.

No open caveats.

## Resolved Caveats

The following table lists the resolved caveats in this release. Click a bug ID to access Cisco’s Bug Search Tool to see additional information about that bug.

Table 3 Resolved Caveats

Bug ID	Description
<a href="#">CSCvt43605</a>	Active Sessions do not represent accurately
<a href="#">CSCvu28159</a>	Retrying baremetal commission fails when initial commission scheduled VMs to other baremetals
<a href="#">CSCvu31581</a>	Not equal filter not working as expected while using CIDR notations for Addresses
<a href="#">CSCvu38850</a>	GET on /openapi/v1/conversations/<id> returns Bad Request - not a valid dimension

<a href="#">CSCvu57323</a>	Add the segmentation workspace consumer and provider filters to the openAPI exported conversations
<a href="#">CSCvu61687</a>	Resque job `RefreshSensorTags` may fail on single agent with improper data
<a href="#">CSCvu69596</a>	Internal services may fail if namenode service goes offline
<a href="#">CSCvs77382</a>	Tetration Virtual Appliance not in sync with UI
<a href="#">CSCvu41066</a>	AIX lw sensor may result in long running process due to number of active connections
<a href="#">CSCvu73952</a>	AIX lw sensor may find hostnames with a trailing NULL character on gui
<a href="#">CSCvs99019</a>	Loss of network connectivity while installing or upgrading windows sensor software on Windows 2019 platform when NPCAP is being installed.
<a href="#">CSCvu16228</a>	Using `Top` CPU quota mode on Tetration agents may cause agent to crash
<a href="#">CSCvu42961</a>	Selecting package in vulnerabilities may result in `backend service error`
<a href="#">CSCvu78800</a>	Package Details may have blank CVE's and/or Affected Workloads
<a href="#">CSCvu82971</a>	Tetration Edge - provide more info to the sysloghost field

## Known Behaviors

- During upgrade when a new RPM is uploaded, adhocKafka is gracefully shut down. This is done to avoid Kafka index corruption. Kafka comes back up after the upgrade. If upgrade is aborted after uploading the RPM, adhocKafka should be restarted using the explore command.

## Compatibility Information

The software agents in the 3.3.2.42 release support the following operating systems (virtual machines and bare-metal servers) for microsegmentation (deep visibility and enforcement):

- Linux:
  - CentOS-6.x: 6.1 to 6.10
  - CentOS-7.x: 7.0 to 7.7
  - Redhat Enterprise Linux-6.x: 6.1 to 6.10
  - Redhat Enterprise Linux-7.x: 7.0 to 7.8
  - Redhat Enterprise Linux-8.x: 8.0 to 8.1
  - Oracle Linux Server-6.x: 6.1 to 6.10
  - Oracle Linux Server-7x: 7.0 to 7.7
  - SUSE Linux-11.x: 11.2, 11.3, and 11.4
  - SUSE Linux-12.x: 12.0, 12.1, 12.2, 12.3, 12.4, 12.5
  - SUSE Linux-15.x: 15.0, 15.1
  - Ubuntu-14.04
  - Ubuntu-16.04
  - Ubuntu-18.04

- Windows Server (64-bit):
  - Windows Server 2008R2 Datacenter
  - Windows Server 2008R2 Enterprise
  - Windows Server 2008R2 Essentials
  - Windows Server 2008R2 Standard
  - Windows Server 2012 Datacenter
  - Windows Server 2012 Enterprise
  - Windows Server 2012 Essentials
  - Windows Server 2012 Standard
  - Windows Server 2012R2 Datacenter
  - Windows Server 2012R2 Enterprise
  - Windows Server 2012R2 Essentials
  - Windows Server 2012R2 Standard
  - Windows Server 2016 Standard
  - Windows Server 2016 Essentials
  - Windows Server 2016 Datacenter
  - Windows Server 2019 Standard
  - Windows Server 2019 Essentials
  - Windows Server 2019 Datacenter
- Windows VDI desktop Client:
  - Microsoft Windows 8
  - Microsoft Windows 8 Pro
  - Microsoft Windows 8 Enterprise
  - Microsoft Windows 8.1
  - Microsoft Windows 8.1 Pro
  - Microsoft Windows 8.1 Enterprise
  - Microsoft Windows 10
  - Microsoft Windows 10 Pro
  - Microsoft Windows 10 Enterprise
  - Microsoft Windows 10 Enterprise 2016 LTSC
- IBM AIX operating system (Alpha):
  - AIX version 7.1
  - AIX version 7.2
- Container host OS version for policy enforcement:
  - Red Hat Enterprise Linux Release 7.1, 7.2, 7.3, 7.4, 7.7
  - CentOS Release 7.1, 7.2, 7.3, 7.4, 7.7
  - Ubuntu-16.04

The 3.3.2.42 release supports the following operating systems for visibility use cases only:

- Linux:
  - CentOS-5.x: 5.7 to 5.11
  - Redhat Enterprise Linux-5.x: 5.7 to 5.11
- Windows Server (64-bit):
  - Windows Server 2008 Datacenter
  - Windows Server 2008 Enterprise
  - Windows Server 2008 Essentials
  - Windows Server 2008 Standard
- Windows VDI desktop Client:
  - Microsoft Windows 7
  - Microsoft Windows 7 Pro
  - Microsoft Windows 7 Enterprise

The 3.3.2.42 release supports the following operating systems for the universal visibility agent:

- Redhat Enterprise Linux 4.0 (32-bit and 64-bit)
- CentOS 4.0 (32-bit and 64-bit)
- Redhat Enterprise Linux 5.0 (32-bit)
- CentOS 5.0 (32-bit)
- Windows Server (32-bit and 64-bit)
- Solaris 11 on x86 (64-bit)
- AIX 5.3 (PPC)

The 3.3.2.42 release supports the following Cisco Nexus 9000 series switches in NX-OS and Cisco Application Centric Infrastructure (ACI) mode:

Table 4 Supported Cisco Nexus 9000 Series Switches in NX-OS and ACI Mode

Product line	Platform	Minimum Software release
Cisco Nexus 9300 platform switches (NX-OS mode)	Cisco Nexus 93180YC-EX, 93108TC-EX, and 93180LC-EX	Cisco NX-OS Release 9.2.1 and later
	Cisco Nexus 93180YC-FX, 93108TC-FX, and 9348GC-FXP	Cisco NX-OS Release 9.2.1 and later
	Cisco Nexus 9336C-FX2	Cisco NX-OS Release 9.2.1 and later
Cisco Nexus 9300 platform switches (ACI mode)	Cisco Nexus 93180YC-EX, 93108TC-EX, and 93180LC-EX	Cisco ACI Release 3.1(1i) and later
	Cisco Nexus 93180YC-FX, 93108TC-FX	Cisco ACI Release 3.1(1i) and later
	Cisco Nexus 9348GC-FXP	Cisco ACI Release 3.1(1i) and later
	Cisco Nexus 9336C-FX2	Cisco ACI Release 3.2 and later
	Cisco Nexus 9500 series switches with N9K-X9736C-FX linecards only	Cisco ACI Release 3.1(1i) and later

## Usage Guidelines

This section lists usage guidelines for the Cisco Tetration Analytics software.

- You must use the Google Chrome browser version 40.0.0 or later to access the web-based user interface.
- After setting up your DNS, browse to the URL of your Cisco Tetration Analytics cluster: <https://<cluster.domain>>

## Verified Scalability Limits

The following tables provide the scalability limits for Cisco Tetration (39-RU), Cisco Tetration-M (8-RU), and Cisco Tetration Cloud:

Table 5 Scalability Limits for Cisco Tetration (39-RU)

Configurable Option	Scale
Number of workloads	Up to 25,000 (VM or bare-metal)
Flow features per second	Up to 2 Million
Number of hardware agent enabled Cisco Nexus 9000 series switches	Up to 100

Note: Supported scale will always be based on which ever parameter reaches the limit first

Table 6 Scalability Limits for Cisco Tetration-M (8-RU)

Configurable Option	Scale
Number of workloads	Up to 5,000 (VM or bare-metal)
Flow features per second	Up to 500,000
Number of hardware agent enabled Cisco Nexus 9000 series switches	Up to 100

Note: Supported scale will always be based on which ever parameter reaches the limit first

Table 7 Scalability Limits for Cisco Tetration Virtual (VMWare ESXi)

Configurable Option	Scale
Number of workloads	Up to 1,000 (VM or bare-metal)
Flow features per second	Up to 70,000
Number of hardware agent enabled Cisco Nexus 9000 series switches	Not supported

Note: Supported scale will always be based on which ever parameter reaches the limit first.

## Related Documentation

The Cisco Tetration Analytics documentation can be accessed from the following websites:

Tetration Datasheets: <https://www.cisco.com/c/en/us/products/security/tetration/datasheet-listing.html>

General Documentation: <https://www.cisco.com/c/en/us/support/security/tetration/tsd-products-support-series-home.html>

The documentation includes installation information and release notes.

Table 8 Installation Documentation

Document	Description
<i>Cisco Tetration Analytics Cluster Deployment Guide</i>	Describes the physical configuration, site preparation, and cabling of a single- and dual-rack installation for Cisco Tetration (39-RU) platform and Cisco Tetration-M (8-RU).  Document Link: <a href="https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/hw/installation_guide/Cisco-Tetration-M5-Cluster-Hardware-Deployment-Guide.html">https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/hw/installation_guide/Cisco-Tetration-M5-Cluster-Hardware-Deployment-Guide.html</a>
<i>Cisco Tetration Virtual Deployment Guide</i>	Describes the deployment of Tetration virtual appliance.  Document Link: <a href="https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/install/b_Tetration_Analytics_Virtual_Appliance_Deployment_Guide.html">https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/install/b_Tetration_Analytics_Virtual_Appliance_Deployment_Guide.html</a>
<i>Cisco Tetration Cluster Upgrade Guide</i>	Document Link: <a href="https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/install/b_Tetration_Analytics_Upgrade_Guide.html">https://www.cisco.com/c/en/us/td/docs/security/workload_security/tetration-analytics/sw/install/b_Tetration_Analytics_Upgrade_Guide.html</a>
<i>Latest Threat Data Sources</i>	<a href="https://updates.tetrationcloud.com/">https://updates.tetrationcloud.com/</a>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2020 Cisco Systems, Inc. All rights reserved.