



Pulse Secure Virtual Traffic Manager: Release Notes

22.1 - 22.7R2

Copyright Notice

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti") and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.lvanti.com.

Copyright © 2024, Ivanti, Inc. All rights reserved.

Protected by patents, see <https://www.ivanti.com/patents>.


Contents

New Features	4
Security Advisory and Patch Updates	9
Product Compatibility	10
Software	10
Containers	10
Cloud Platforms	10
Hardware Platforms	10
Virtual Appliance Editions	10
Large Objects in the Webcache	12
GeoIP database	13
Support for software running on RHEL/CentOS 6	14
Fixed Issues and Other Changes	15
Known Issues	23
Upgrade Instructions	24
Documentation	25
Technical Support	26
Revision History	27

New Features

Release 22.7R2

The following table describes the major features that are introduced in this release.

Major Features in 22.7R2
Support for life cycle management features for nSA platform integration With this feature enabled, upon integration with nsa platform, vTM can be rebooted, restarted and upgraded or rollback from nsa admin UI.
Pulse Secure Virtual Web Application Firewall Features
<p>The Traffic Manager will install version 4.10-7 of Pulse Secure Virtual Web Application Firewall (vWAF). Version 4.10-0 included a number of important internal updates, including migrating the codebase to Python 3.</p> <p>Before upgrading from version 4.9-x to version 4.10-x, users must ensure that any Python scripts they have included in script libraries are compatible with Python 3.</p> <hr/> <p> Resource Requirements now includes a recommendation that virtual appliances running vWAF should have a RAM allocation of at least 4GB. Version 4.10-x of vWAF should be expected to consume approximately 500MB more system RAM than previous versions.</p>

Release 22.7R1

The following table describes the major features that are introduced in this release.

Major Features in 22.7R1
Support for vTM analytics on nSA Platform (Preview). This enables vTM to export analytics data to nSA platform.
Pulse Secure Virtual Web Application Firewall Features
<p>The Traffic Manager will install version 4.10-11 of Pulse Secure Virtual Web Application Firewall (vWAF). Version 4.10-0 included a number of important internal updates, including migrating the codebase to Python 3.</p> <p>Before upgrading from version 4.9-x to version 4.10-x, users must ensure that any Python scripts they have included in script libraries are compatible with Python 3.</p>



[Resource Requirements](#) now includes a recommendation that virtual appliances running vWAF should have a RAM allocation of at least 4GB. Version 4.10-x of vWAF should be expected to consume approximately 500MB more system RAM than previous versions.

Release 22.6R1

The following table describes the major features that are introduced in this release.

Pulse Secure Virtual Web Application Firewall Features

The Traffic Manager will install version 4.10-10 of Pulse Secure Virtual Web Application Firewall (vWAF). Version 4.10-0 included a number of important internal updates, including migrating the codebase to Python 3.

Before upgrading from version 4.9-x to version 4.10-x, users must ensure that any Python scripts they have included in script libraries are compatible with Python 3.



[Resource Requirements](#) now includes a recommendation that virtual appliances running vWAF should have a RAM allocation of at least 4GB. Version 4.10-x of vWAF should be expected to consume approximately 500MB more system RAM than previous versions.

Release 22.5R1

The following table describes the major features that are introduced in this release.

Pulse Secure Virtual Web Application Firewall Features

The Traffic Manager will install version 4.10-9 of Pulse Secure Virtual Web Application Firewall (vWAF). Version 4.10-0 included a number of important internal updates, including migrating the codebase to Python 3.

Before upgrading from version 4.9-x to version 4.10-x, users must ensure that any Python scripts they have included in script libraries are compatible with Python 3.



[Resource Requirements](#) now includes a recommendation that virtual appliances running vWAF should have a RAM allocation of at least 4GB. Version 4.10-x of vWAF should be expected to consume approximately 500MB more system RAM than previous versions.

Release 22.3R1


The following table describes the major features that are introduced in this release.

Report Number	Features	Description
VTM-45316, RFE-1580	OAuthv2.0 Authorization	OAuth 2.0 authorization framework along with openID is supported in traffic manager which enables user to provide session based restricted access to backend services using OAuth workflow.
VTM-46013	Traffic Manager as an ingress point	Traffic Manager as an ingress point for Kubernetes infrastructure, and to control Traffic Manager configuration through standard Kubernetes mechanisms.
VTM-45571, RFE-1417	JWT TrafficScript support for parsing, validation, and generation of JWS tokens in a secure way by GUI based key management system	New TrafficScript functions have been provided to parse, validate and generate JWT tokens. Support is only for JWS tokens and supports algorithms HS256, HS384, HS512, RS256, RS384, RS512, ES256, ES384, and ES512.

Release 22.2

The following table describes the major features that are introduced in this release.


Report Number	Features	Description
VTM-45466, RFE-1417, SR34618	JWT TrafficScript support for parsing, validation, and generation of JWS tokens	New TrafficScript functions have been provided to parse, validate and generate JWT tokens. Support is only for JWS tokens and supports algorithms HS256, HS384, HS512, RS256, RS384, RS512, ES256, ES384, and ES512.
Pulse Secure Virtual Web Application Firewall Features		

Report Number	Features	Description
		<p>The Traffic Manager will install version 4.10-7 of Pulse Secure Virtual Web Application Firewall (vWAF). Version 4.10-0 included a number of important internal updates, including migrating the codebase to Python 3.</p> <p>Before upgrading from version 4.9-x to version 4.10-x, users must ensure that any Python scripts they have included in script libraries are compatible with Python 3.</p> <hr/> <p> Resource Requirements now includes a recommendation that virtual appliances running vWAF should have a RAM allocation of at least 4GB. Version 4.10-x of vWAF should be expected to consume approximately 500MB more system RAM than previous versions.</p>

Release 22.1

The following table describes the major features that are introduced in this release.

Report Number	Features	Description
VTM-43929, RFE-1449	Update Appliance base operating system to Ubuntu 20.04	<p>The base operating system of the appliances has been updated to Ubuntu 20.04.3. This ensures Ubuntu standard support until April 2025 for the operating system components.</p> <p>The following appliance form factors have their base OS changed: Docker, VMWare vSphere, Microsoft Hyper-V, KVM, Amazon EC2, Microsoft Azure, Google Cloud Engine and Bare Metal Server. Citrix Xen appliance with the updated OS is not published as part of this release. This will be included in a future release.</p> <p>There are no changes in the installation or upgrade procedures for the on-premise or cloud virtual appliances. Installation procedure using PXE boot has changed, where the installation ISO image needs to be served through a web server. Please refer to the "Appliance Image Installation and Getting Started Guide" for more information.</p>

Report Number	Features	Description
VTM-45384, VTM-45355	Base64URL Encode/Decode	Support for a new TrafficScript function <code>string.base64urlencode()</code> has been added which helps in encoding a given input to a URL and filename safe base64URL format. Added support for TrafficScript function <code>string.base64urldecode()</code> which can be used for base64URL decoding.
Pulse Secure Virtual Web Application Firewall Features		
<p>The Traffic Manager will install version 4.10-7 of Pulse Secure Virtual Web Application Firewall (vWAF). Version 4.10-0 included a number of important internal updates, including migrating the codebase to Python 3.</p> <p>Before upgrading from version 4.9-x to version 4.10-x, users must ensure that any Python scripts they have included in script libraries are compatible with Python 3.</p>		
<p> Resource Requirements now includes a recommendation that virtual appliances running vWAF should have a RAM allocation of at least 4GB. Version 4.10-x of vWAF should be expected to consume approximately 500MB more system RAM than previous versions.</p>		

Security Advisory and Patch Updates

Ivanti has released security advisories and mitigations for critical vulnerabilities in the Pulse Secure Virtual Traffic Manager. For more information on the security aspects of network setup, see [System Security](#). Ivanti recommends you read this chapter carefully before setting up live services.

The following CVE's have been fixed:

CVE's	Ivanti Forum links
CVE-2024-7593	For more details, see Ivanti forum .

Product Compatibility

You can install and use this product version on the following platforms:

Software

- Linux x86_64: Kernel 3.10 - 5.13, glibc 2.17+

For Route Health Injection: ncurses 5 (libncurses.so.5, libtinfo.so.5)

Containers

- Docker: 1.13.0 or later recommended

Cloud Platforms

- Amazon EC2 - as a virtual appliance or native software install
- Microsoft Azure - as a virtual appliance
- Google Compute Engine - as a virtual appliance or native software install

Hardware Platforms

- Bare Metal Server - for information on qualified servers, see the Pulse Secure Virtual Traffic Manager Hardware Compatibility List at <https://www.ivanti.com/support/product-documentation>



Beginning with Release 21.4 and later, you cannot create a bootable USB drive.

Virtual Appliance Editions

- VMware vSphere 6.5, 6.7, 7.0, 8.0
- Microsoft Hyper-V Server 2016
- Microsoft Hyper-V under Windows Server 2016 and 2019
- QEMU/KVM (RHEL/CentOS 7.x; Ubuntu 18.04, 20.04)

Resource Requirements

Virtual appliances should be allocated a minimum of 2GB of RAM. Virtual appliances running Pulse Secure Virtual Web Application Firewall should be allocated a minimum of 4GB of RAM.

For a virtual appliance upgrade to succeed, a minimum of 2.7GB must be available on the /logs partition. To confirm the available free disk space, use the **System > Traffic Managers** page of the Admin UI.

Large Objects in the Webcache

A Traffic Manager running version 20.1 or later will be unable to store objects greater than 2GB in the web cache, even if the web cache is enabled and all cacheability conditions are met. If you rely upon this feature, please contact Technical Support through the usual support mechanism (see [Technical Support](#)).

GeolP database

VTM-43072, RFE-1472 The database used by the Traffic Manager to look up the geographic location of incoming requests based on their IP address was removed from the software installation package and appliance images in version 20.3 in order to better comply with various privacy protection laws. This database is used when performing Global Load Balancing, when displaying the Activity Map or using the geo.* TrafficScript functions.

Update packages containing the most recent version of this database can be obtained from the [Ivanti customer portal](#). To download navigate to *Downloads > Select Security > Ivanti vADC > Sign in > Downloads > Pulse Secure Virtual Traffic Manager > Related Software > geoip_update_20240301.tgz*. The database present in existing appliances or installations that are upgraded to this version will be copied into the new traffic manager installation and will continue to be used until an update package with a newer database is applied. VTM-43072, RFE-1472



The GeolP database already present in Traffic Manager instances that are upgraded to this version is retained, and continues to be used until an update package with a newer database is applied.

Support for software running on RHEL/CentOS 6

VTM-43879 Version 20.3 was the last release to support 2.6.32-based kernels or glibc 2.12. Versions from 21.1 onwards require kernel version 3.10 or later, and glibc 2.17 or later, as described in [Product Compatibility](#).

In particular, this means that it is not possible to install version 21.1 or later on a RHEL/CentOS 6 system, or to upgrade an existing Traffic Manager instance on RHEL/CentOS 6 to version 21.1 or later.

Fixed Issues and Other Changes

The following table lists issues that have been fixed and are resolved by upgrading to the named release.

Release 22.7R2

Report Number	Description
Security	
VADC-297	Fixed a security issue CVE-2024-7593 related to interface that exposes the administrator UI.
Upgrade and Rollback	
VTM-46572	Fixed upgrade issue in hardware appliances.
VTM-46569	Updated documentation to include a warning statement

Release 22.7R1

Report Number	Description
Security	
VTM-46435	Fixed an issue which could lead to heap buffer overflow as mentioned in CVE-2023-4863.
Fault Tolerance	
VTM-45925	upgrading a vTM cluster from a lower version to a higher version, you may see a warning that the traffic managers have different configuration versions. This means that some of the configuration settings are not consistent across the cluster. This is fixed by ensuring that all the vTMs in the cluster have the same configuration.

Pulse Secure Virtual Web Application Firewall

Report Number	Description
WAF	
PRS-417235	Fixed the issue by code changes related to Python 3 generated by vWAF.
PRS-417596	Fixed the issue by enabling modification of telemetry config via existing REST API generated by vWAF.

Release 22.6R2

Report Number	Description
Security	
VADC-297	Fixed a security issue CVE-2024-7593 related to interface that exposes the administrator UI.

Release 22.6R1

Report Number	Description
Administration Server	
VTM-46271	Fixed an UI related issue which didn't give enough information on how to add multiple email addresses for alerting events. Both comma and space can be used as delimiter now as per UI info.
Security	
VTM-46220	Fixed a security issue CVE-2022-4304 related to openssl.

Pulse Secure Virtual Traffic Manager Appliance

The following table lists issues that have been fixed and are resolved by upgrading to this release.

Report Number	Description
Cloud Platforms	
VTM-46273	Fixed an issue which could lead to IPv4 associations being not displayed properly when vTM software version is installed on AWS CentOS 7.

Pulse Secure Virtual Web Application Firewall

Report Number	Description
WAF	
PRS-415852	Fixed the issue by enabling the Logrotator for all the log files generated by vWAF.

Release 22.5R2

Report Number	Description
Security	
VADC-297	Fixed a security issue CVE-2024-7593 related to interface that exposes the administrator UI.

Release 22.5R1

Report Number	Description
Installation and Upgrading	
VTM-46236	Fixed an issue which could lead to upgrade failure from a version with new version format to any other version.
Configuration	
VTM-46226	Fixed an issue where TIP becomes unconfigurable if VA is restored without machine specific information

Report Number	Description
Administration Server	
VTM-46055	Fixed the radio button in "Event from" section which even after selecting "Some Pools" couldn't retain the selection.
VTM-46053	The fix is to reflect the bind IP properly in UI and configuration files when it's changed from UI so that user can still access GUI smoothly post modification.
SNMP	
VTM-45911	Fixed an issue which gives a wrong picture about the available free memory in the system
TrafficScript	
VTM-43956	Fixed an issue which could lead to unexpected memory reservation for trafficscript data_size

Pulse Secure Virtual Traffic Manager Appliance

The following table lists issues that have been fixed and are resolved by upgrading to this release.

Report Number	Description
Virtual Appliance	
VTM-46218	Fixed a customer specific issue which could lead to interface name shuffling post upgrade.

Pulse Secure Virtual Web Application Firewall

Report Number	Description
WAF	
WAF-1156 (PRS-414746)	Handled the exceptions ReadTimeout and increased the request timeout second.
WAF-1117	Internal Security Improvement. Baseline updated with CVE-2021-44228.

Report Number	Description
WAF-1151	WAF Debug binary is now available for 4.10.0006, 4.10.0007, 4.10.0008. Modified the CxFreeze (open source) code to generate debug binary

Release 22.3R3

Report Number	Description
Security	
VADC-297	Fixed a security issue CVE-2024-7593 related to interface that exposes the administrator UI.

Release 22.3R2

Report Number	Description
Security	
VTM-34418	In vTM, to store the user passwords SHA256 is used now instead of MD5.
VTM-45907	For vWAF component of vTM, the zlib version is upgraded to 1.2.12. The older version of zlib (1.2.11) allows memory corruption when deflating (i.e.,when compressing) if the input has many distant matches.

Release 22.3R1

Report Number	Description
Security	
VTM-45908	Upgraded nghttp2 to 1.49.0 which fixes several security issues. CVE-2020-11080,CVE-2019-9511,CVE-2019-9513

Report Number	Description
VTM-45907	Upgraded curl and curl-nss to 7.84.0 which fixes several security issues. CVE-2021-22945,CVE-2021-22946,CVE-2021-22947,CVE-2021-22897,CVE-2021-22898,CVE-2021-22901,CVE-2021-22876,CVE-2021-22890,CVE-2020-8286,CVE-2020-8285,CVE-2020-8284,CVE-2020-8231,CVE-2019-15601,CVE-2019-5481,CVE-2019-5482,CVE-2019-5435,CVE-2019-5436,CVE-2018-16890,CVE-2019-3822,CVE-2019-3823,CVE-2018-14618,CVE-2018-0500,CVE-2018-1000300,CVE-2018-1000301
VTM-45899	Upgraded libpng to version 1.6.37 which fixes CVE-2019-7317
VTM-43673	Upgraded gorilla websocket to version 1.5.0 which fixes CVE-2020-27813
Performance	
VTM-45892	Update OpenSSL to version 1.1.1q with fixes for CVE-2022-1292, CVE-2022-2068 & CVE-2022-2097
Connection Processing	
VTM-45301	Modified the documentation for traffic script function pool.use() to reflect that it may not resolve a hostname to a reachable IP address.

Release 22.2

Report Number	Description
Security	
VTM-45643	Upgraded kernel version to 5.4.0-107-generic which fixes the security issue CVE-2022-27666.

Pulse Secure Virtual Traffic Manager Appliance

The following table lists issues that have been fixed and are resolved by upgrading to this release.

Report Number	Description
Virtual Appliance	

Report Number	Description
VTM-45635	Addressed the initial network setup issue, when there is no DHCP setup.

Pulse Secure Virtual Web Application Firewall

No changes in this release.

Release 22.1

Report Number	Description
Performance	
VTM-45449	Update OpenSSL to version 1.1.1n to be compliant with the latest security updates.
SOAP API	
VTM-45387	The version of the expat XML parser library used by the Administration Server to provide its SOAP API has been upgraded to 2.4.6, addressing CVE-2022-25235, CVE-2022-25236, CVE-2022-25313 - CVE-2022-25316, CVE-2022-22822 - CVE-2022-22827, CVE-2021-46143, CVE-2021-45960, CVE-2022-23990 and CVE-2022-23852.
VTM-45333	The version of the expat XML parser library used by the Administration Server to provide its SOAP API has been increased to 2.4.4, addressing CVE-2022-22822 - CVE-2022-22827, CVE-2021-46143, CVE-2021-45960, CVE-2022-23990 and CVE-2022-23852.
TrafficScript	
VTM-45321	The Perl Compatible Regular Expression library (PCRE) has been updated to version 10.39.
Connection Processing	
VTM-38103	Fixed an issue where the Admin UI displayed timeout options only applicable to TCP connections for UDP protocol based virtual servers.
SSL/TLS and Cryptography	

Report Number	Description
VTM-45399	Fixed an issue where SAN extension was missing in SSL self-signed certificates.
VTM-38496, VTM-17444	Decreased the time needed for the SSL Decryption page of the Admin UI to be generated if many SSL certificates are installed.

Pulse Secure Virtual Traffic Manager Appliance

The following table lists issues that have been fixed and are resolved by upgrading to this release.

Report Number	Description
Virtual Appliance	
VTM-45565	Fixed an issue where the bonding device could not be configured correctly due to an error in the identifying the device.
VTM-44975	Fixed an issue which prevented the utility for expanding logs partition from executing again in case it failed for first time.

Pulse Secure Virtual Web Application Firewall

The following table lists issues that have been fixed and are resolved by upgrading to this release.

Report Number	Description
WAF-1114	Fix a unicode decoding error.
WAF-1116	Fix a string decoding error.
WAF-1128	Upgrade libexpat and Python.
WAF-1128, VTM-45472, VTM-45554	Upgrade OpenSSL to 1.1.1n.

Known Issues

The following table lists the Known issues in release 22.1 - 22.7R2.

Report Number	Report	Description
VTM-34654	KVM Network Interface Card renaming	In rare circumstances a KVM host may change the PCI addresses of a virtual appliance's network cards after a reboot, resulting in the network interface labels changing. This can be fixed by removing the configuration from the non-existent card on the traffic manager 'Networking' page and re-adding it to the correct card.
VTM-38881	Obsolete counters are missing from old REST API versions	Obsolete counters removed from version 6.0 of the status API are missing in versions 5.X, despite the schemata published with the product claiming they are still present.

Upgrade Instructions

To learn more about upgrading your Traffic Manager, see the [Pulse Secure Virtual Traffic Manager: Installation and Getting Started Guide](#) applicable to your product variant.

Documentation

Ivanti documentation is available at <https://www.ivanti.com/support/product-documentation>.

For policy reasons, security issues are not normally mentioned in release notes. To find more information about our security advisories, see the [security advisory](#) page on the Ivanti website.

Technical Support

Full support for version 22.7R2 will be available for three years from the release date of 26 May, 2024.

Full support for version 22.1 will be available for one year from the release date of 21 April, 2022.

For more information, see the End of Support and End of Engineering Schedule notices at the following location:

https://forums.ivanti.com/s/article/Product-End-of-Support-End-of-Engineering-Schedule-Pulse-Secure-Traffic-Manager-vTM?language=en_US&psredirect

For additional information or assistance, contact Ivanti Support Center:

- <https://forums.ivanti.com/s/contactsupport>
- support@ivanti.com

For technical support resources, browse the Technical Support website

<https://forums.ivanti.com/s/contactsupport>.

Revision History

The following table lists the revision history for this document:

Revision	Revision Date	Description
9.0	19th August, 2024	Updated the Fixed Issues list with CVE-2024-7593 for Release 22.3R3, 22.5R2, 22.6R2.
8.0	13th August, 2024	Added the Security Advisory and Patch Release section with the list of fixed CVE's.
7.0	26th May, 2024	Revisions for release 22.7R2
6.0	23rd January, 2024	Revisions for release 22.7R1
5.0	14th October, 2023	Revisions for release 22.6R1
4.0	18 July, 2023	Revisions for release 22.5R1
3.0	15 October, 2022	Revisions for release 22.3R1
2.0	July, 2022	Revisions for release 22.2.
1.0	21 April, 2022	Release 22.1 release Notes created.