TeraVM Classic Release Notes

TeraVM Classic Release 14.7

Help and Support

TeraVM User Documentation, Online Training Guides and Videos are available on the documentation portal: https://avcomm.viavisolutions.com/login-account

For support queries, please log a call on the http://wirelesssupport.viavisolutions.com

For accounts, please contact your local VIAVI Account Representative. You can also contact support using the mail alias for your region:

Location	Email
China	TeraVMSupport.CN@viavisolutions.com
EMEA	TeraVMSupport.EMEA@viavisolutions.com
North America	TeraVMSupport.USA@viavisolutions.com
Japan	TeraVMSupport.JP@viavisolutions.com
Korea	TeraVMSupport.KO@viavisolutions.com
South East Asia	TeraVMSupport.SG@viavisolutions.com
India	TeraVMSupport.IND@viavisolutions.com

Copyright

End User License Agreement

The usage of the TeraVM product and documentation is subject to the Viavi Solutions Ireland Limited standard Software Licence Agreement, which is available at TeraVM License Agreement.

Please read the terms of the Software Licence Agreement carefully before using the documentation.

Notice

Every effort was made to ensure that the information in this manual was accurate at the time of printing. However, information is subject to change without notice, and VIAVI reserves the right to provide an addendum to this manual with information not available at the time that this manual was created.

Terms and Conditions

Specifications, terms, and conditions are subject to change without notice. The provision of hardware, services, and/or software are subject to the VIAVI standard terms and conditions, available at www.viavisolutions.com/terms.

Table of Contents

Chapter 1. What's New in this Release

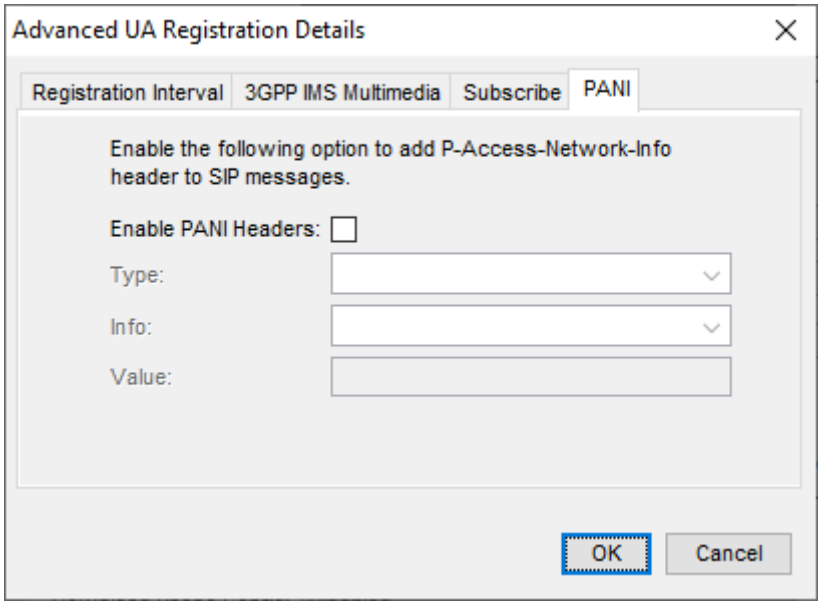
The following sections detail what is new in this release.

1.1 Java Client

The following section contains the changes made to the TeraVM Java Client for this release.

1.1.1 PANI Information in SIP Messages

From this tab you can access and configure the P-Access-Network-Info header. There are three user configurable values for PANI that can be added to SIP messages, they are: Type, Info, Value.



The following is an example of values entered into the PANI tab fields:

- **Type:** 3GPP-GERAN
- **Info:** utran-cell-id-3gpp
- **Value:** 44050221100C2A02

With these values entered, then the fields are added to requests and responses as follows:

```
P-Access-Network-Info: 3GPP-GERAN; utran-cell-id-3gpp=44050221100C2A02
```

Note that in line with the 3GPP spec TS 24.229, there are exceptions to which requests and responses it can be added to. Also, the initial unprotected REGISTER when Secure VoLTE is enabled will not contain the P-Access-Network-Info header field.

1.1.1.1 Substituting Configured Values

When the PANI fields are configured it is possible to substitute the configured values by specifying the substitutions in any additional headers.

- {panitype}
- {paniinfo}
- {panival}

P-Access-Network-Info: {panitype}-X; {paniinfo}={panival}

Which would result in the following:

```
P-Access-Network-Info: 3GPP-E-UTRAN-X; utran-cell-id-3gpp=44050221100C2A02
```

1.1.2 VoIP IMS AKA SIP Signalling

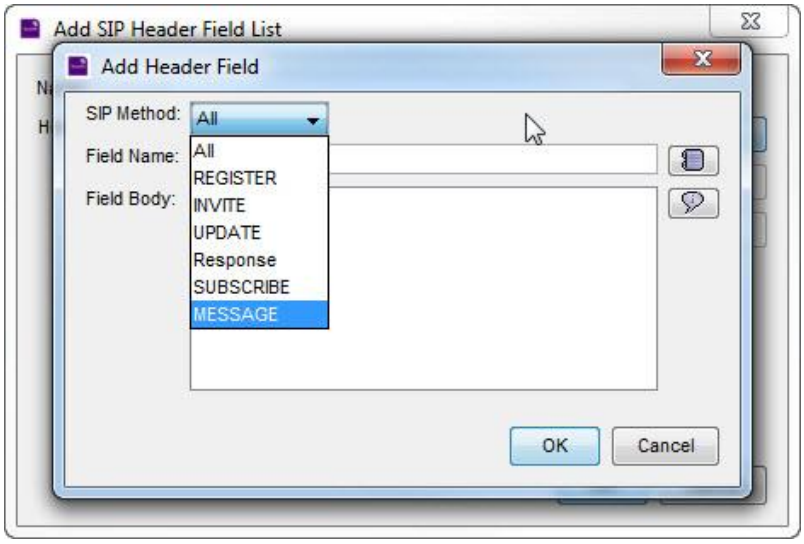
Support is provided for generating SIP Messages with simple content between TeraVM VoIP UAC and TeraVM VoIP UA(s) applications. SIP Messages with a simple signalling flow can be generated with a plain text body between TeraVM VoIP and UAS applications. The following is an example SIP Message with a plain text body:

```
MESSAGE sip:123456789@example.com SIP/2.0

Via: SIP/2.0/UDP 10.0.0.10:5060;branch=z9hG4bK1101497358

Max-Forwards: 70

To: <sip:123456789@example.com>

From: <sip:client-a@10.0.0.10>;tag=1638928616

Call-ID: 351213069 2@10.0.0.10

CSeq: 12868 MESSAGE

User-Agent: diversifEye/SIPUA

Content-Length: 24

Content-Type: text/plain

Hello this is message one
```

1.1.2.1 SIP Header Lists

A new SIP Method **MESSAGE** is included to allow user defined SIP Header Fields.

1. From the test Groups tab select the SIP Header Filed Lists tab and right click to Add SIP Header Field List. *The Add SIP Header Field List dialog opens.*
2. Click Add.
3. Click the SIP Method drop-down and select **MESSAGE**.

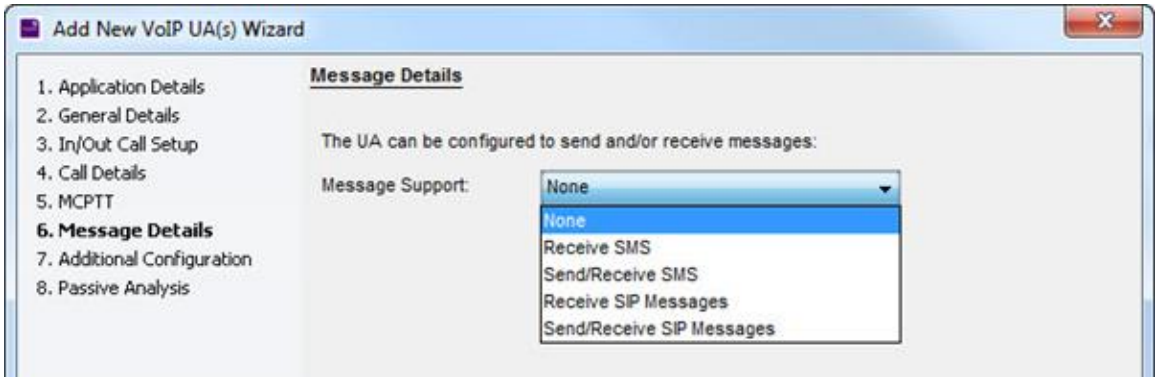


4. Create the message as required, using the **Field Body** text input for the content of the SIP Header.

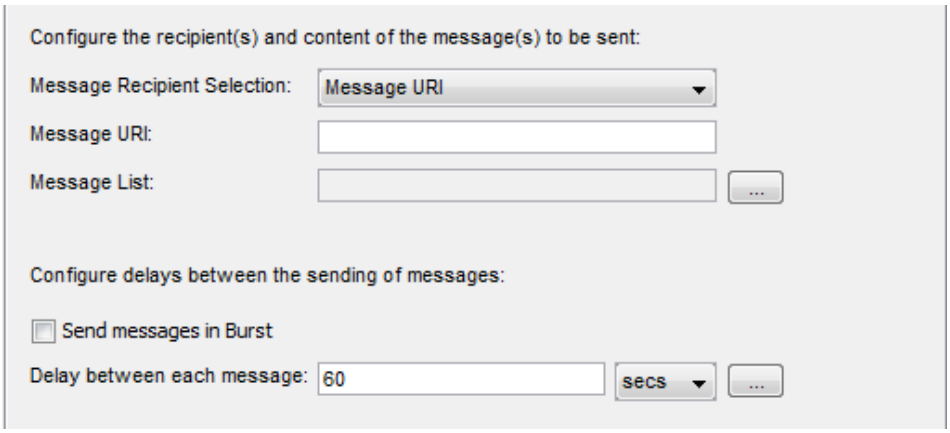
1.1.2.2 Add New VoIP Wizard

When adding a new VoIP UA(s) application, the new options are found at **6. Message Details > Message Support** drop-down box.

- **None**: default
- **Receive SIP Messages**: receive only with no further options in wizard step.
- **Send/Receive SIP Messages**: wizard step changes to allow recipient and content of the message to be sent.



The following image shows the fields available when the **Send/Receive SIP Messages** is selected in the Message Support drop-down. For more details on feature and parameters, see the TeraVM Java Client User Guide.



1.1.3 EdDSA Requirements for TLS and IKEv2

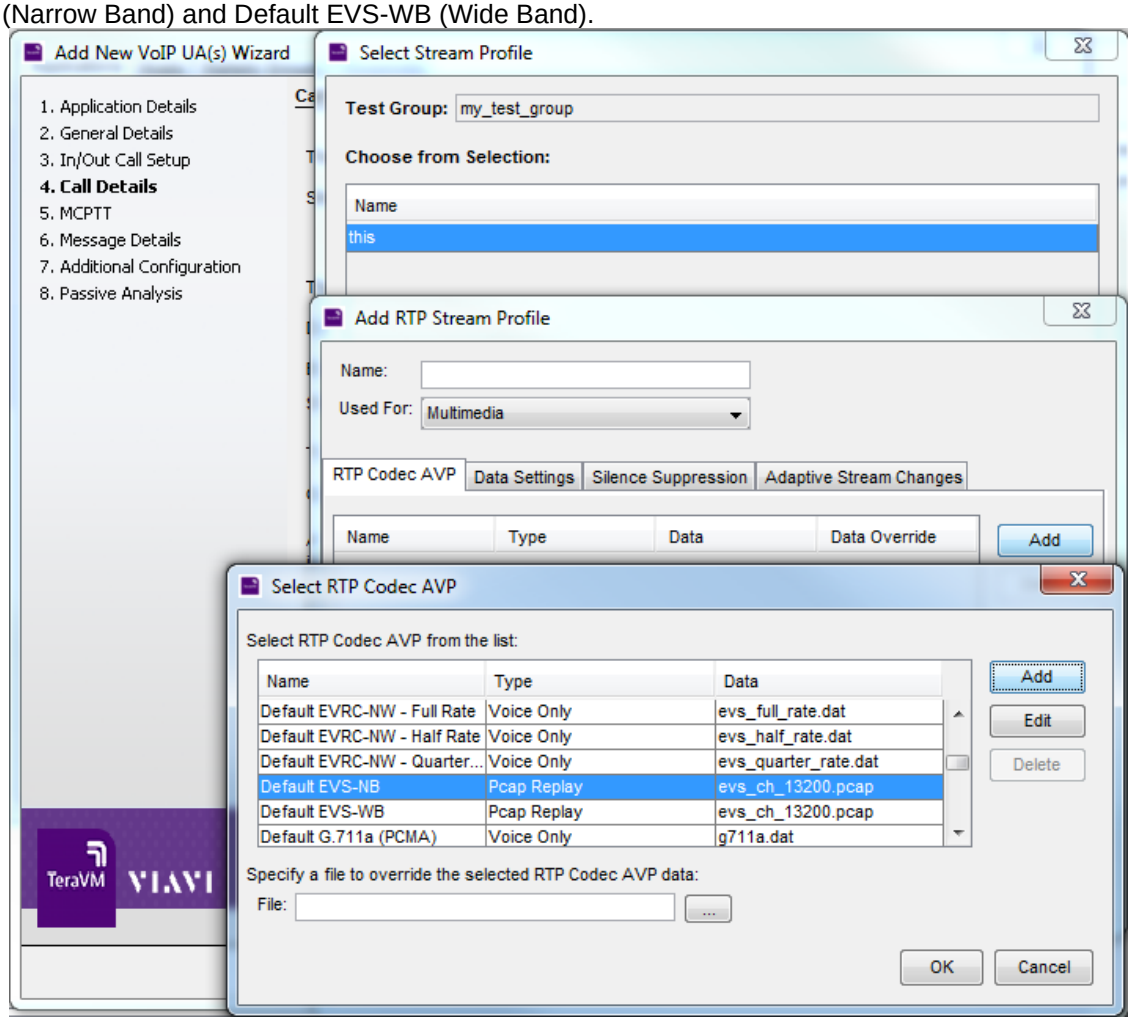
TeraVM IKE and AnyConnect VPN clients support authentication using certificates with Edwards-curve Digital Signature Algorithm (EdDSA) over IPSec and AnyConnect TLS tunnels. An authentication hash value can be calculated using an EdDSA signature scheme and the authentication payload. User supplied certificates using either of the supported EdDSA instances of Ed25519, or Ed448, are used accordingly during the authentication process with the server of the connecting user. Supported EdDSA instance details:

• **Ed25519**: EdDSA variant using 32 bytes public keys, producing 64 byte signatures. Provides 128-bit equivalent security.

• **Ed448**: EdDSA variant using 57 byte public keys and producing 114 byte signatures. Provides 224-bit equivalent security.

1.1.4 Support for EVS Codec and Rate Control

VoIP applications now support Enhanced Voice Services (EVS) Codecs which can be selected as an RTP Stream Profile when configuring a VoIP UA. Two EVS Codecs are provided: Default EVS-NB (Narrow Band) and Default EVS-WB (Wide Band).



The Adaptive Bit Rate Level List includes the EVS codec which has the following list levels.

Table 1-1. EVS NB Default Bit Rates

Level	Bit Rate
1	5.9
2	7.2
3	8.0
4	9.6
5	13.2
6	16.4
7	24.4

Table 1-2. EVS WB Default Bit Rates

Level	Bit Rate
1	5.9
2	7.2
3	8.0
4	9.6
5	13.2
6	16.4

7	24.4
8	32.0
9	48.0
10	64.0
11	96.0
12	12.0

The EVS codec is a variable rate codec that allows dynamic switching between rates depending on network conditions. This is so that if bandwidth is limited it can switch to a lower bit rate.
When switching to a new bit rate the first 50 packets will contain the CMR byte. After that the stream will revert to the Compact Format header.

1.1.5 CSRF Support in Clientless VPN

TeraVM Clientless VPN supports CSRF tokens for login and logout operations. When the Clientless VPN is connecting to a Cisco ASA it is checked for CSRF tokens, if detected the tokens will be stored and used for login and logout. If there are no CSRF tokens present, then the login and logout operations will ignore CSRF token validation.

1.1.6 Support for MCPTT KPIs

TeraVM now supports MCPTT service Key Performance Indicators (KPIs) 1 to 4 as defined in 3GPP TS 22.179. The KPI statistics 1, 2, 4 will be automatically reported for a VoIP UA which is MCPTT enabled. They will not be present for a VoIP UA which is not MCPTT enabled or any other VoIP applications.

KPI 3 is measured with VoIP Latency Statistics for any client receiving RTP audio packets. All the members of the calling group, and the all members of the callee group, must have the **Enable Latency Statistics** checked.

If **Passive Analysis** is enabled the Latency Statistics will not be collected. For each MCPTT Group or Private Call all the VoIP UAs can have either Passive Analysis Statistics or Latency Statistics, but not both. There cannot be a mix of UAs on a call with one or the other of these statistics types enabled.

Latency Statistics can be enabled in the VoIP UA(s) Wizard, or properties, from the *Additional Configuration* step **Statistics button.**

Enable Latency Statistics no longer has a dependency on **Allow UA Initiate Calls** to be selected.

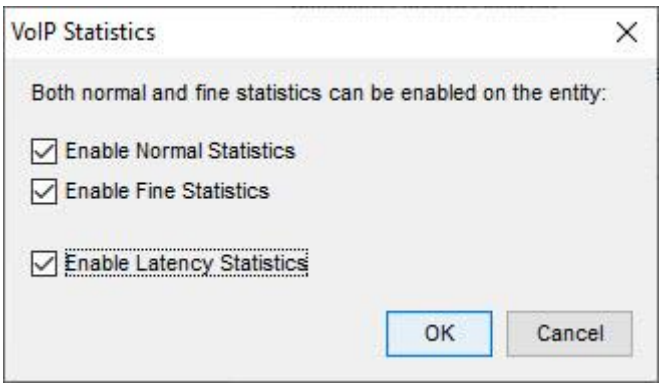


Table 1-3. Supported MCPTT KPIs

KPI	Definition	Validation
KPI-1	MCPTT Access time	Measure of time it takes between sending an initial floor request and receiving a floor granted response.

KPI-2	End-to-end MCPTT Access time	Measure of time it takes to send an INVITE and send the final ACK message.
KPI-3	Mouth-to-ear latency	Measured with VoIP latency stats for any client receiving RTP audio packets.
KPI-4	Late call entry performance	Measure of time it takes to receive an INVITE message and receive the first RTP audio packet.

1.2 TeraVM HTML5 Client

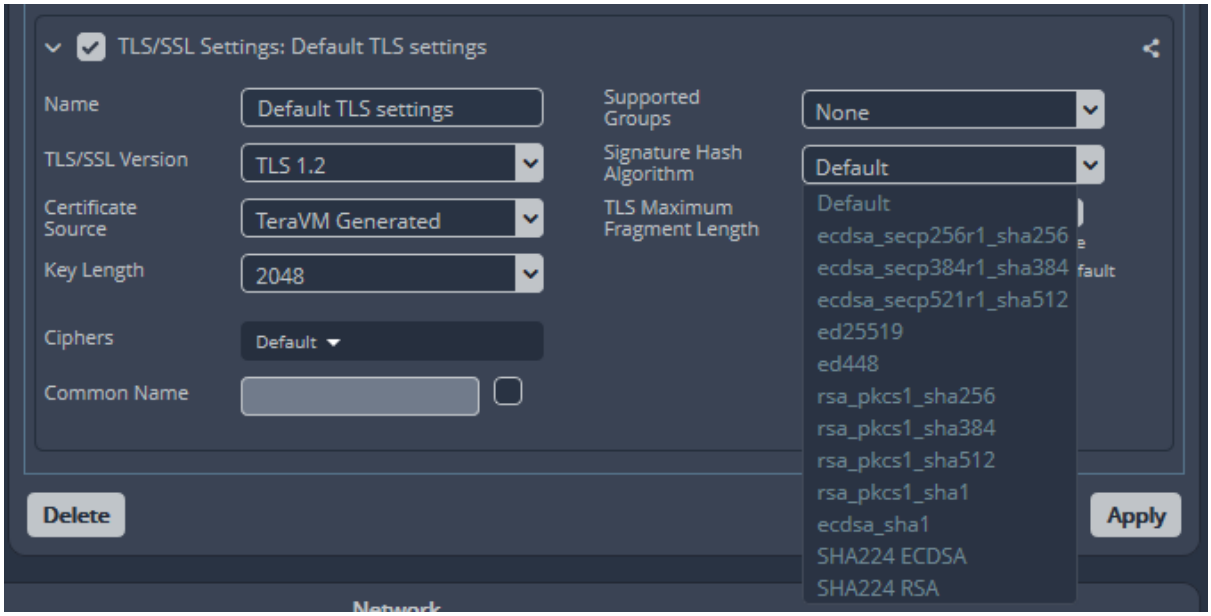
The following section contains the changes made to the TeraVM HTML5 Client for this release.

1.2.1 Server-Side TLS Settings Configuration

The **Signature Hash Algorithm** field is added to the TLS/SSL Settings in tests, Application Mix > Application Settings, that use TLS 1.2 or TLS 1.3. TLS 1.2 and 1.3 signature algorithms extensions allow Clients to signal supported and preferred signature algorithms and hash functions. When using an SUT in TeraVM, the **TLS Signature Hash Algorithm** field can be used to ensure that both Client and Server uses the expected signature algorithm.

For TLS 1.3, the algorithm options available are: **Default**, **ecdsa_secp256r1_sha256**.

For TLS 1.2, the algorithms options are shown in the following image.



1.3 Other Changes

This section includes changes made that are outside of those already covered.

1.3.1 ESXi Orchestration Default Memory Increase

The default memory allowance for CPU and JVM settings of the TeraVM Controller are adjusted to increase performance of scaled testing. These settings are not applicable for upgrade scenarios. The new values are:

New Default VM settings:

- Memory: 16GB
  - memoryMB = memoryAllocation.limit = memoryAllocation.reservation = 16000
- Number of CPUs
  - numCpus = numCoresPerSocket = 2

Settings in TVM-C Guest OS:

- JVM Max Heap Megabytes: 10000
  - wrapper.java.additional.3=-Xmx10000m

The changes to the VM settings and JVM do not apply to upgrades, the existing setup will not be updated. The VM settings above will be applied automatically to all non-RDA TeraVM Classic TVM-Cs being deployed.

The TVM-C diversifEye JVM Max Heap size will be adjusted to 0.625 of the TVM-C VM memory.

The TVM Memory will also be used to automatically adjust the memory assigned to our traffic generator.

The automatic TVM-C JVM settings can be overridden via a new VmProp settings in vmutil.cfg, vmcJvmMaxHeapMegabytes will allow the automatic JVM heap setting described above to be overridden by the user.

For increased memory tests, please review the additional Performance Global Settings in TeraVM_VMWare_ESXi_Setup_Guide.pdf.

The new default VM settings (16GB RAM, 2CPUS) for TVM-C are not applicable for upgrades.

Chapter 2. Release Compatibility

This section contains changes between this release and the last release.

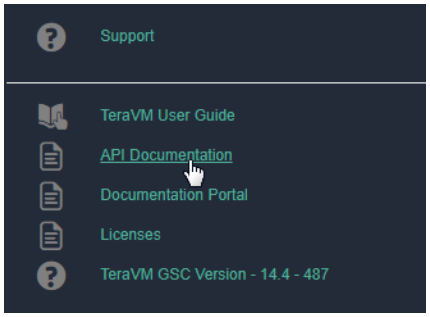
2.1 New Test Names in 14.7

No new tests were added in this release.

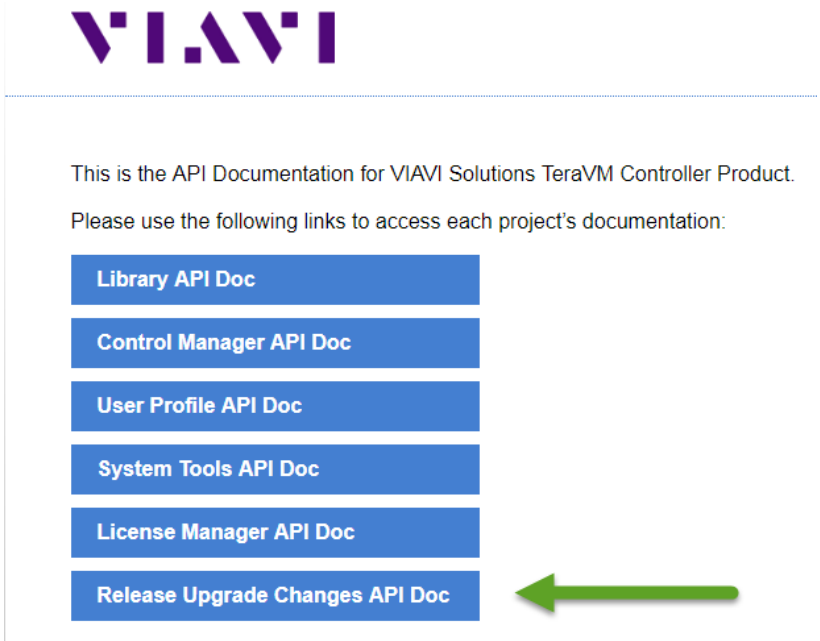
2.2 REST API Changes

Detail about the changes made to the REST APIs can be found at the API Documentation web page.

1. From TeraVM Controller, either Workspace or Library, click the help icon and select the API Documentation. *The Documentation Landing page opens.*



2. From the Landing page select *Release Upgrade Changes API Doc* button, shown below.



3. Select the link that details the changes you want to see. *The Changes to Release page opens.*

Chapter 3. Patches

In the case where you need to apply a patch from VIAVI, please use the steps that follow. All previous patches between the last and current release are included in this release.

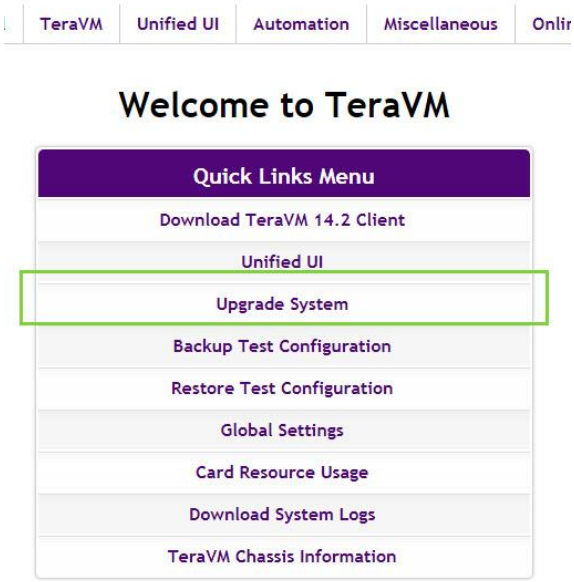
3.1 Installing a Patch

Use this procedure to install a patch using the Web Administration Interface.

1. Download the patch from the relevant folder. Close any open TeraVM user interfaces and stop any tests.
2. In your browser, enter the IP address of the Executive/Controller.
3. Enter your User Name and Password and click **Sign In**.
4. Select **Utilities**.
5. From the *Welcome to TeraVM* page, select **Upgrade System** and login using:

   User Name: **driverAdmin**
   Password: **diversifEye**

Figure 3-1. Welcome to TeraVM



6. Select the **Choose File** button.
7. Select the appropriate patch file and click **Open**.
8. Click **Upload**. The file uploads in several seconds.
9. Click **Upgrade** and wait for the patch to complete upgrading.

Chapter 4. Upgrading to this Release

As a general guideline, when upgrading to a new version of TeraVM, deploy the new TeraVM Management Assistant (TeraVM MA) and remove the previous version. The TeraVM MA is used for deploying new Test Modules, and when moving from TeraVM 11.4, it is used to deploy a TeraVM Executive.

To use the Streamlined Upgrade Process, see *4.4 Streamlined Upgrade Process.* Otherwise, use the following sequence of actions for the upgrade:

Required Upgrades

- TeraVM Executive (TeraVM) – see Section 4.3.1 Download and Install Upgrade. If your upgrading from 11.4, then you must deploy an Executive from the new TeraVM MA see the TeraVM VMWare ESXi Setup Guide for more information.
- TeraVM Controller (TeraVM and d500/d1000) – see Section 4.3.1 Download and Install Upgrade.
- Delete the old Test Modules and then redeploy new Test Modules (TeraVM) – see the relevant platform setup guide.
- Upgrade Off Controller Repository (if using an Off Controller Repository) – see Section 4.2 Upgrading Off Controller Repository.

Optional Upgrades

- Cybersecurity (TeraVM).

For more release specific guidelines, you must follow the conditions below and refer to the appropriate TeraVM Setup Guide for your platform.

Important: You must check to see if your upgrade process is impacted by any of the following conditions.

Installation Conditions

- **Centralized Executive Upgrade**

  If you are using a Centralized Executive and planning to upgrade, ideally all your Executives should be upgraded to the same version or at least the Central Executive is the newest.

- **Upgrading from 13.1**

  If upgrading from 13.1 to 13.2 or, 13.3, 13.4, 13.4.1, 13.4.2, 14.0, 14.1 you must follow the upgrade procedure from Section 3.1, for both the Controller and the Executive. This is to ensure that you do not encounter a timeout while upgrading them.

- **Pre-12.0 Introduction of TeraVM Executive**

  TeraVM 12.0 was a major release, with many new features and architectural changes to the product. Therefore, if you are migrating from a pre-12.0 release, you must deploy the TeraVM Test Modules and the TeraVM Executive to use TeraVM successfully.

- **Pre-12.1 to Post 12.1: Authentication Service**

  If upgrading from a pre-12.1 to post 12.1 release, you will see the message The Authentication Service from the Executive Machine Could Not Be Reached. To get around this, in the browser, you must amend the TeraVM Controller IP with :8181. For example: http://TVM-C IP:8181.

- **12.1 Security Certificate Required**

  When upgrading from pre-12.1 to post-12.1 and trying to reach the Executive or Controller via the browser, the browser displays a connection not secure dialog. This dialog will differ from browser to browser. You must add an exception to accept a security certificate before you can log into the Executive or Controller. You will also need to do this the first time that you open Pool Manager from the UI.

- **Upgrade to Off Controller Repository**

  13.1 release includes performance improvements to the Off Controller Client Repository. If you have a have an installed Off Controller Client Repository, then use the procedure in Section 3.2 to perform the upgrade. TeraVM supplies a separate Client Repository which can be of unlimited size, external to the Controller (Off Controller). It comes as a separate virtual machine, and must be downloaded separately. The repository is sized at 32 GB by default. You can increase this by adding disks in vSphere (you cannot remove or resize existing disks).

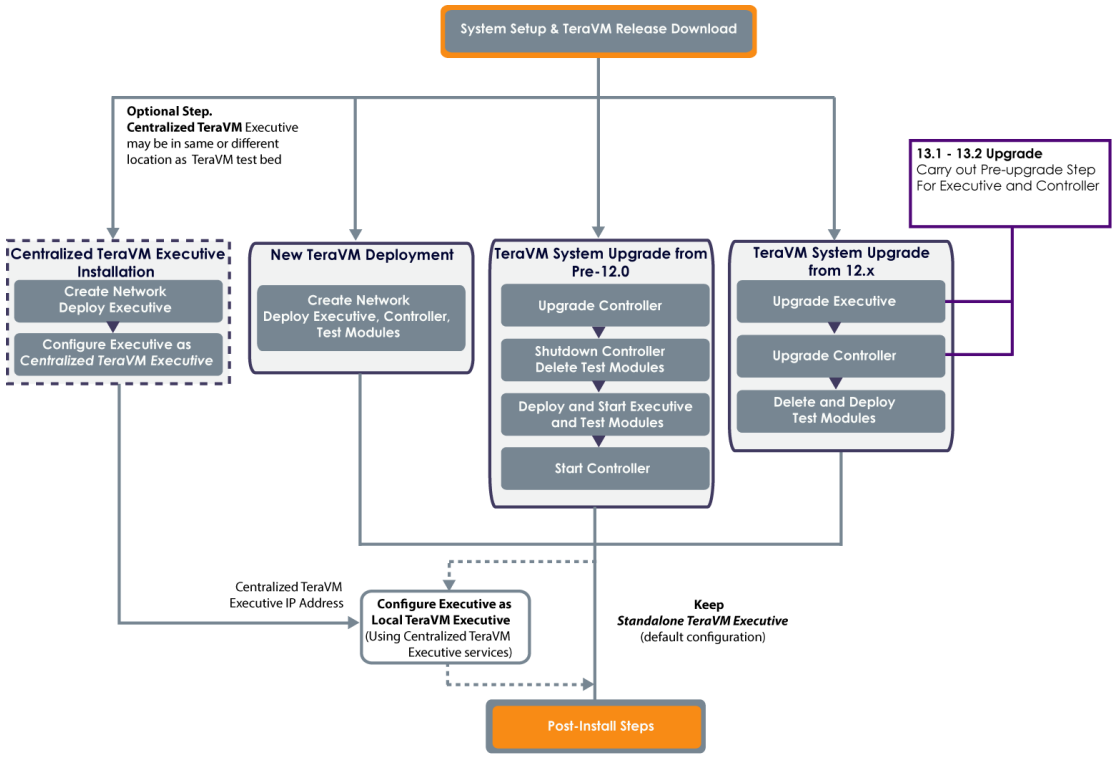
- **Cybersecurity Updates**

  This release includes the addition of ETPro files, these files are only supported from TeraVM Controller version 13.3-4267 and onward.

  When you perform this upgrade, all Cybersecurity Updates from the last Cybersecurity upgrade will be removed. Please download the latest Cybersecurity updates and reboot your controller before reinstalling. Contact support for details. This only applies if you have purchased the additional Cybersecurity Database license from VIAVI.

An overview of the TeraVM install and upgrade process is shown below. For details on installing or upgrading to this release, please see the relevant hypervisor/cloud guide.

Figure 4-1. Installing or Upgrading to this Release



4.1 Upgrade from 13.1 Pre-Upgrade Step

This procedure must be done for both the TeraVM Executive and Controller before upgrading from TeraVM 13.1 to 13.2 or,13.3, 13.4, 13.4.1, 13.4.2, 14.0, 14.1.

Prerequisite

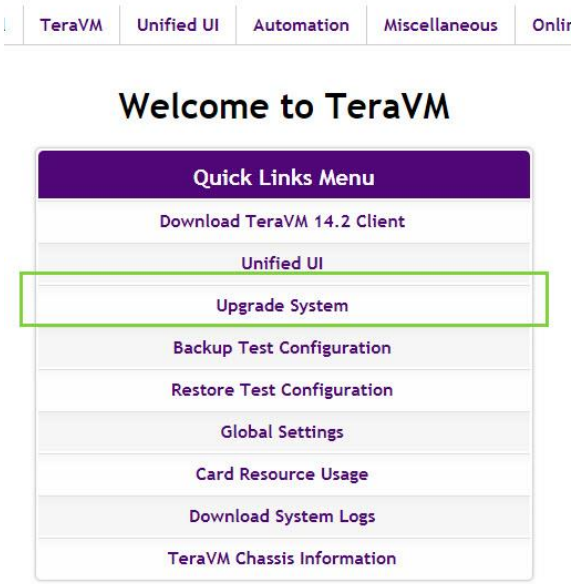
- Failure to follow this procedure during an upgrade will lead to a timeout or an error message. This will not negatively impact the upgrade, but you must follow this procedure and apply the pre-upgrade steps.

1. In your browser, enter the IP address of the Executive/Controller.
2. Enter your User Name and Password and click **Sign In**.
3. Select **Utilities**.
4. From *the Welcome to TeraVM* page, select **Upgrade System** and login using:

   Username: **diverAdmin**

   Password: **diversifEye**

Figure 4-2. Welcome to TeraVM



5. Select the **Choose File** button.
6. Select the appropriate pre-upgrade file and click **Open**.

   TeraVM_Controller-13.2_preupgrade-98134-upload.tgz
   TeraVM_Executive_1.6_preupgrade-98132-upload.tgz

7. Click **Upload**. The file uploads in several seconds.
8. Click **Upgrade**.
9. After the pre-upgrades have been completed continue with the Executive and Controller upgrades as normal.

4.2 Upgrading Off Controller Repository

Use this procedure to upgrade the Off Controller Client Repository. The following conditions apply to the upgrade process.

- When upgrading TeraVM to 13.4.2 release, the pcaps stored on the Off Controller Client Repository are deleted. For upgrades to post 13.4.2 release, the pcaps are not deleted.
- The Client Repository Off Controller versions older than 1.5-525 will not work with the TeraVM version 13.4.2 or higher. When upgrading TeraVM to 13.4.2 you must also upgrade the Client Repository Off Controller to the 1.5-525 version.

Note
If you are upgrading an Off Controller Repository deployed from 1.3-329 ova and you encounter the error message: <unable to validate signature>, please contact support.

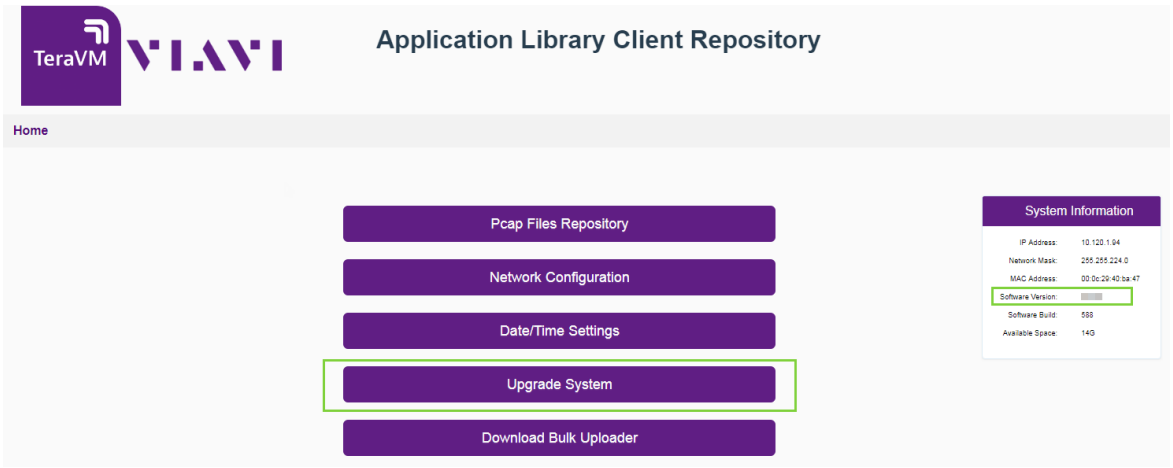
Prerequisites

- This procedure assumes you have a correctly installed Off Controller Client Repository.
- Check the Off Controller is supported in the following Supported Off Controller Repository table.

1.2-161	1.3-329	1.4-417
1.5-525	1.6-550	1.7-650

1. Download the Client Repository Off Controller Upgrade file from the release folder > Upgrade folder: ClientRepositoryOffController_Upgrade-_upload.tgz.
2. In the vSphere Client ensure that the Client Repository Off Controller is powered on.
3. In the vSphere Client select the Client repository Off Controller and note its IP Address from the Summary tab in the **General** pane.
4. Enter the IP Address in your browser and make a note of the Software Version displayed under the System Information.

Figure 4-3. Application Library



5. Select **Upgrade System**. *The Upgrade System page opens*.
6. Click **Browse** and select the Off Controller Client Repository Upgrade file that you previously downloaded.
7. Click **Upload**. *When completed, a file uploaded message is displayed.*

8. Click **Upgrade**.
    - An error is displayed in your browser. **Please note** that this is expected behaviour.
    - If the error states **<unable to validate signature>** please contact support.
    - Check the IP Address of the Client Repository Off Controller, it may have changed.
9. Enter the IP Address of the Client Repository in the browser and check the **Software Version** under the System Information panel. *The Software Version has incremented.*

4.3 Check Your Current Versions against Upgrade Installer

The Upgrade installer can be used in conjunction with the versions listed below. If the release you are currently using is not listed, please contact VIAVI support.

Attention: If you are upgrading from a release prior to 11.0, please contact VIAVI support as you may need to run an additional step.

Release versions use the following convention: `”Major.Minor-BuildNumber” or “X.Y-Build”

Where X represents the major version, Y the minor version.

Table 4-1. Controller Releases Supported by Installer

11.0-257	11.0.1-259	11.1-300
11.2-334	11.2.1-339	11.3-379
11.3.1-401	11.3.2-420	11.4-613
12.0-1454	12.0.1-1692	12.0.2-1961
12.0.2-1996	12.0.3-2053	12.0.2-2030
12.1-3090	12.1-3110	12.1.1-3121
12.1.2-3152	13.0-3297	13.1-3699
13.1-3703	13.2-3946	13.2.1-4090
13.3-4261	13.3-4267	13.3.1-4289
13.3.2-4488	13.3.3-4502	13.4-4623
13.4.1-4645	13.4.2-4707	13.4.3-4718
14.0-5096	14.0-5106	14.0-5113
14.0.1-5118	14.0.2-5163	14.1-5432
14.1.1-5609	14.1.2-5527	14.1.3-5238
14.2-5819	14.2.1-5826	14.3-6124
14.3-6150	14.3.1-6228	14.4-6324
14.4.1-6439	14.4.2-6395	14.5-6605
14.6-6812	14.7-7021	

Table 4-2. Executive Releases Supported by Installer

1.0	1.1	1.2
1.3	1.4	1.5
1.6	1.7	1.7.2
1.8	1.9	1.9.1
1.9.2	1.9.3	1.10
1.11	1.16	1.17
1.18	1.19	1.20
1.21		

4.3.1 Download and Install Upgrade

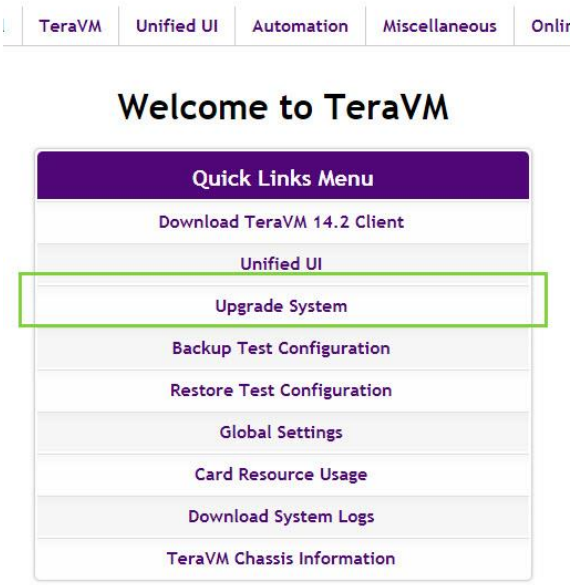
Use this procedure to install an upgrade using the HTML5 interface.

Installing an Upgrade

1. Download the upgrade from the location provided by VIAVI support. Close any open TeraVM user interfaces and stop any tests.
2. In your browser, enter the IP address of the Executive/Controller.
3. Enter your User Name and Password and click **Sign In**.
4. Select **Utilities**.
5. From the *Welcome to TeraVM* page, select **Upgrade System** and login using:

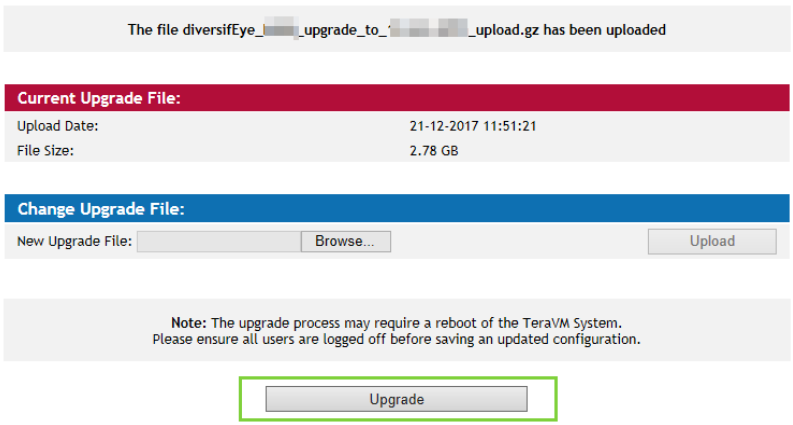
   User Name: **diverAdmin**
   Password: **diversifEye**

Figure 4-4. Welcome to TeraVM



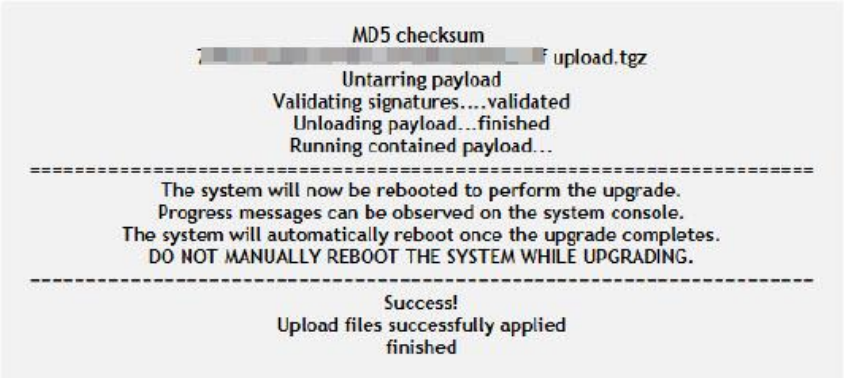
6. Select the **Choose File** button.
7. Select the appropriate patch file and click **Open**.
8. Click **Upload** and wait until the file has uploaded.

Figure 4-5. Upload File



9. Click **Upgrade** and wait for the patch to complete upgrading.

Note: The controller reboots twice during the upgrade procedure. The upgrade progress can be followed using the Console on the VM or connecting to the Console on a physical system (d500/d1000). If the system updates successfully, a message similar to the following appears:



10. Otherwise, a message will appear with instructions about how to ftp the upgrade file to the system. Follow these instructions to complete the upgrade step.

    Note: Older hardware may require ftp. Contact VIAVI support if you run into issues.

11. If you are a TeraVM Cybersecurity user and have not already updated to the latest Cybersecurity Database, note that this is an extra step in the upgrade process. For further details, contact VIAVI Support.
12. Next, continue to the relevant platform set up guide, for example, VMWare EXSi, to deploy the TeraVM Test Modules and Executive.

4.4 Streamlined Upgrade Process

Use this procedure to upgrade from TeraVM 14.0 and upward. You can also use the script for upgrades from TeraVM 11.4, but you must manually deploy a TeraVM Executive first and power it on before running the script. This script considers for upgrade all the TeraVM Virtual Machines that are powered on and on the same Comms network. The Upgrade TeraVM Testbed script is available from TeraVM 14.0.

> **Note**
> The Streamlined Upgrade Process is only applicable on a TVM-630 or a testbed on 1 server with only 1 TVM-E.

Table 4-3. Supported TeraVM Controller Versions

11.4-613	11.4-618	13.0.3927	13.3-4261
13.3-4267	13.4-4623	13.4.2-4707	14.0-5096
14.0-5106	14.0-5113	14.0.1-5118	14.0.2-5163
14.1-5432	14.1.1-5609	14.1.2-5527	14.1.3-5238
14.2-5819	14.3-6124	14.3-6150	14.3.1-6228
14.4-6324	14.4.1-6439	14.4.2-6395	14.5-6605
14.6-6812	14.7-7021		

1. Check that you are upgrading from a Supported TeraVM Controller Version.
2. In the vSphere Client, right-click the TeraVM MA and select **Open Console**, if it is not already open. *The TeraVM Management Assistant Opens.*
3. From the icons displayed on the TeraVM Management Assistant desktop, double-click the **03 Upgrade TeraVM Testbed** icon. The Upgrade TeraVM Testbed script runs. Enter parameters as prompted:

```
upg>TeraVM Upgrade Script upgrade.pl-0.01...

upg>Using VMware-Perl-Sdk-5.5.0... upg>Using perl-v5.18.4...

upg>Reading config settings from: "/usr/local/share/perl5/diversifEye/Upgrad
e/upgrade.cfg"...

ESXi Host IP Address/Hostname[10.110.1.11]: 10.110.1.11

ESXi Host Username[root]: root

ESXi Host Password[Password1234]: Password1234

IP Address or VM Name of TVM-E[10.110.2.22]: 10.110.2.22
```

4. Press **Enter** to accept the default empty values for the following:

```
TVM-E User[teravm]:

TVM-E Password[teravm]:
```

5. A connection is established to the ESXi Host IP Address/Hostname, enter **y** to continue.

```
upg>Connecting to: "10.110.1.11"...

upg>WARNING: OAUTH is apparently not supported by the TVM-E at: "10.110.2.22

"! Assuming no token is necessary for access to the testbed...
```

```
Upgrading TeraVM Testbed on ESXi Host: 10.110.1.11...

VM            From                To            Upgrade

TVM-E-001     1.7.2-1672          1.9-1893      Yes

TVM-C-001     13.4-4623           14.0-4998     Yes

TVM-2-003     3.0.39-1248         3.0.49-1473   Yes

TVM-2-004     3.0.39-1248         3.0.49-1473   Yes

Proceed with upgrade(y|true|n|false)[yes]:y
```

6. The upgrade script automatically upgrades the TeraVM Controller and changes and deploys the Test Modules.

```
Final Upgrade Status:

Name        State     Sec Phase    Log

TVM-E-001   OK         949

TVM-C-001   OK       2438

TVM-2-003   OK       701

TVM-2-004   OK       210


upg>All VMs upgraded OK.

upg>Disconnecting from: "10.110.1.11"...

Type ENTER to dismiss:
```

7. The upgrade is complete, press **Enter** to dismiss.

Chapter 5. Platforms

This chapter details the supported: certified hardware, hypervisors, operating systems and web browsers.

5.1 Hardware Platforms

The matrix below shows which hardware TeraVM has been certified on.

Table 5-1. Certified Hardware

Cisco UCS		DELL	
Model	***NIC***	***Model***	***NIC***
C240	Cisco VIC 1285 and 1385 PCIe Ethernet NIC (40Gig)	R640	Intel X550 Dual Port 10G Base-T
			Intel X710 Dual Port 10Gb
			Broadcom (1G)
C220	Cisco Systems Inc VIC 1225 PCIe Ethernet NIC (10Gig)	R630	Intel 82599EB 10-Gigabit SFP
			Intel 10-Gigabit X540-AT2
			Broadcom (1G)
		R620	Intel 82599EB 10-Gigabit SFP
			Broadcom (1G)

5.2 Hypervisors

This release has been tested with the following hypervisors and versions (AWS, XEN and Azure platforms are tested with major releases):

Table 5-2. Hypervisors

Hypervisor	Hypervisor Version	TVM Version	TVM Types	vSwitch Types	Executive Version	Virtual NIC
ESXi‡	ESXi 5.5_U1 and U3 ESXi 6.5_U2†	3.0.95	See ‡	VMXNET3	1.21	VMware VMXNET3 virtual interface

† The Dell R640 support requires VMware ESXi 6.5 U2 Dell EMC Customized A04 and CISCO Custom Image for ESXi 6.5U2 GA.

‡ Additional ESXi Information

- ESXi supports TVM-2 to TVM-5, TVM-7, TVM-8 and TVM-16.
    - TVM-7 is supported for VPN applications only.
    - TVM-8 and TVM-16 are for use with Mellanox Cards. They require a minimum version of ESXi of 5.5.0. Unlike other Test Module types which have only one core for interrupt processing, TVM-8 and TVM-16 use half of their cores for control.
- ESXi supports both Direct Path/DPIO and virtual switch configurations.
- You can now specify a solid-state drive when deploying TeraVM.
- TeraVM is now also tested with ESXi version 6.0 and 6.5 but is not fully certified in performance tests.

5.3 Virtual Machine Requirements

The following table shows TeraVM Virtual machine CPU and Memory requirements.

Virtual Machine	CPU	Memory
TeraVM Controller	2 vCPU	16 GB
TeraVM Executive	2 vCPU	4 GB
TVM-1	1	2.5 GB
TVM-2	2	2.5 GB
TVM-3	3	5 GB
TVM-4	4	7.5 GB
TVM-5	5	10 GB
TVM-7	7	15GB
TVM-8	8*	17.5GB
TVM-16	16*	37.5GB

*Generally, Test Modules use one core for interrupt handling, and the rest for traffic generation. However, TVM-8 and TVM-16 only use half of their CPU cores for traffic generation, the rest is for interrupt handling.

5.4 Operating System

The following table shows the operating systems that TeraVM Java Client has been tested with.

Table 5-3. Operating Systems

Operating System	Version
Windows	7,8,10
Fedora (32-bit)	22

5.5 Web Browsers

TeraVM is developed to work with modern web browsers that support HTML5.The following table shows the web browsers that TeraVM has been tested with. VIAVI will make every reasonable effort to support older versions.

Table 5-4. Web Browsers

Browser	Version
Mozilla Firefox	68
Internet Explorer	11
Google Chrome	76

Chapter 6. Bugs Fixed and Known Issues

This chapter details any bugs fixed or known issues at the time of the release.

6.1 Bugs Fixed

The following defects were addressed in this release. For further details, please contact VIAVI support.

Table 6-1. Bugs Fixed in this Release

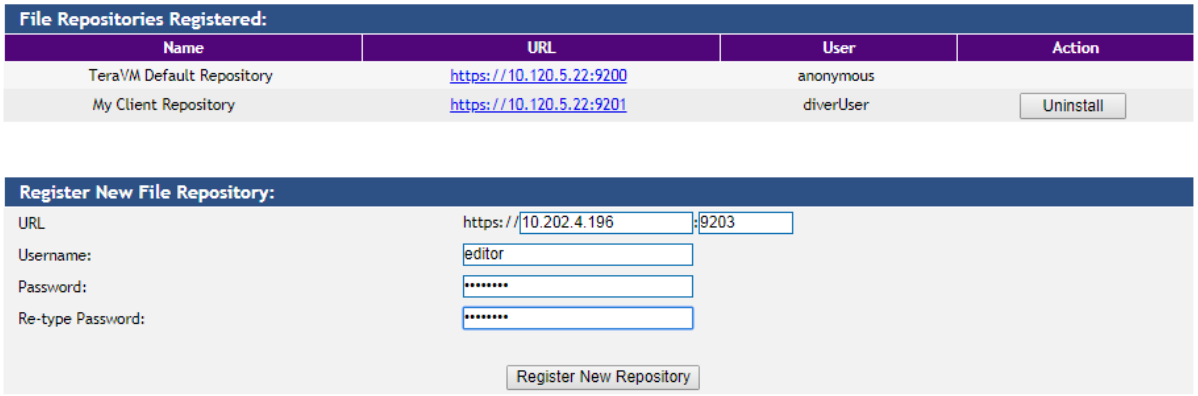
Bug Number	Description
TER-8084	Windows 10 Support not listed in Release Notes for TeraVM Java Client
TER-8086	HTTP HTTPs test causes buffer overflow error HTTP header length exceeds 64K
TER-8108	Pulse Secure VPN tunnels fail after upgrade from version 12.0.2 to 14.5
TER-8211	NTP daemon can die over time even with reliable clock source
TER-8292	Vmutil password uninitialized deploying TVM-C only
TER-8322	[GCP] MLIPS logs are not captured in Controller syslog
17947	using the web interface to change the Maximum JVM size, sets the Initial Size too

6.2 Known Issues

These are the known issues in this release. For further details, please contact VIAVI support.

6.2.1 Difficulty Connecting to UI When Using Pcap Repo

If you encounter difficulties connecting to the UI and you are using Pcap Repos, ensure the connection details are still valid for the Repo, if not unregister and re-register the Repo.



6.2.2 TeraVM Executive Connectivity Lost

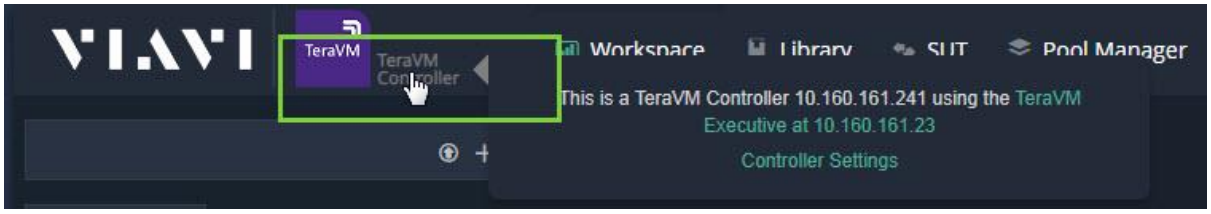
An issue may occur when connectivity to a TeraVM Executive has been lost and the TeraVM Executive needs reconnecting with the TeraVM Controller, but you are not prompted to do so on TeraVM Controller UUI login. Where this occurs use the following procedure.

Setting the Executive IP Address

A new **Controller Settings** link can be accessed under the logo on the TeraVM Controller. This setting improves the accessibility for setting a new Executive IP Address. This feature can be used if you want to quickly set a new Executive IP address.

To change the Executive IP Address:

1. Click the **TeraVM Controller** link next to the logo, in your TeraVM Controller UUI, to open the **Controller Settings** dialog box.



2. Enter the Executive IP Address in the IP Entry Field and click **Set IP**.

3. In ESXi vSphere client, restart the TeraVM Executive and TeraVM Controller.
4. The new Executive IP is set.

6.2.3 Transitioning from Primary to Failover Licence Server

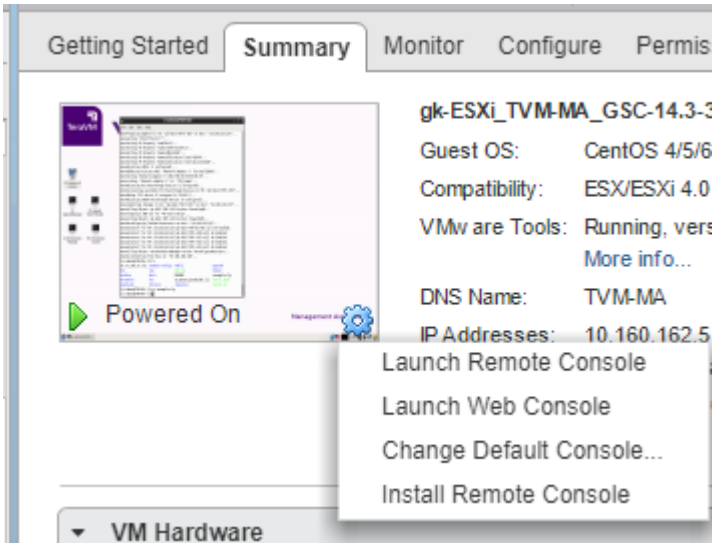
Transitioning from Primary to Failover Licence Server can take approximately 2 minutes. If you have a test running while transitioning then you will see no interference with the test, but if you start a test before the transition is complete the test will fail to start. But once the transition is complete the test will start as normal.

6.2.4 Missing Buttons from Java Client GUI

If you are using more than 100% text size, please be aware that some items on the UI may not be visible. Reduce to 100% and if the issue persists then please contact support.

6.2.5 MA Console Does Not Always Open

Along with VMWare we recommend that when using the ESXi Console on the MA, please select the Remote Console option instead of the Web Console option, as shown in the following image.


Getting Started
Summary
Monitor
Configure
Permis
gk-ESXi_TVM-MA_GSC-14.3-3
Guest OS:
CentOS 4/5/6
Compatibility:
ESX/ESXi 4.0
VMware Tools:
Running, vers
More info...
DNS Name:
TVM-MA
IP Addresses:
10.160.162.5
Powered On
Launch Remote Console
Launch Web Console
Change Default Console...
Install Remote Console
VM Hardware

Appendix A: TeraVM Documentation Set

All TeraVM Guides are available for download at the TeraVM documentation portal:

http://ats.aeroflex.com/login-account

The complete TeraVM documentation set is listed below.

Table 6-2. TeraVM User Guides

User Guides	Description
Release Notes	New features / Changes in the latest release. (Includes supported versions).
TeraVM HTML5 User Guide	TeraVM overview includes setting up and running tests in the HTML5 UI, Centralized Test Library.
TeraVM Java Client User Guide	How to create and run tests in the Java Client: Details of applications and hosts supported. There are also separate application notes for Citrix ICA, SIP trunking and EoGRE.
TeraVM CLI User Guide	Using the Automation Interface (CLI, Perl commands and RFC scripts) for testing. Also man pages are available for commands and scripts in the Documentation sub-directory *cli*.
TeraVM Appliance Set Up Guide	TeraVM Hardware Appliance Set Up (Appliance Customers only).
TeraVM vRAN User Guide	Combined NG4T / VIAVI solution for RAN, Core and Peripheral IP Emulation for 4G.
TeraVM Licensing Guide	How to set up and configure licensing features, e.g. set up license servers and license reporting.
TeraVM Application Library Test Configuration Guide, Application Library Repository Users Guide	Traffic generation test solution for creating application flows. Includes repository setup information.

Table 6-3. Hypervisor/Cloud Specific TeraVM Setup Guides

Hypervisor/Cloud Environment	Document Name
ESXi	TeraVM on VMWare Set Up Guide
KVM	TeraVM on KVM Set Up Guide
OpenStack on KVM	TeraVM on OpenStack Set Up Guide
Citrix XenServer	TeraVM on Citrix Xen Set Up Guide
Hyper-V	TeraVM on Hyper-V Set Up Guide
Amazon AWS	TeraVM on Amazon AWS Set Up Guide
Microsoft Azure	TeraVM on Microsoft Azure Set Up Guide

Table 6-4. TeraVM Reference Guides

Reference Guides	Description
TeraVM Metrics Guide	Statistics/Metrics available with TeraVM
CLI Reference Guides (under Documentation/ cli).	Man pages are available for commands and scripts in the Documentation sub-directory.

For further information please contact:

VIAVI Solutions:

www.viavisolutions.com/wirelessvalidation