



Network Application Performance Management

1. GENERAL
 - 1.1 Service Definition
 - 1.2 Standard Service Features
 - 1.3 Customer Responsibilities
2. SUPPLEMENTAL TERMS
 - 2.1 Country Related Limitations
 - 2.2 Customer Data
 - 2.3 License Grant
 - 2.4 License Restrictions
 - 2.5 Authorized User Registration
 - 2.6 Disclaimer
3. SERVICE LEVEL AGREEMENT
4. FINANCIAL TERMS
 - 4.1 Administrative Charges
 - 4.2 Optional Change Management
 - 4.3 IP Addresses
5. DEFINITIONS

1. GENERAL

- 1.1 **Service Definition.** Network Application Performance Management + (Network APM) monitors the performance of Customer's application environment, from the physical servers and operating systems (either directly or virtually associated to server hardware) to the application processes residing on the host operating systems, subject to country or market availability. Network APM is available at Customer Sites where third parties provide transport service(s), subject to Verizon's written approval.
- 1.2 **Standard Service Features.** Network APM has the following feature options: a) Network APM–Server (also referred to as Network APM- Infrastructure Management), b) Network APM–Application Monitoring, and c) Network APM- End User Experience Monitoring. Customer may choose to implement any or all feature options, as well as various sub features within each main feature. The management levels available for each feature option are described below.
 - 1.2.1 **Network APM – Server.** Verizon will monitor the Managed Devices, Customer Equipment and other systems on the Customer Network on which Customer's applications reside. The devices, server hardware or operating systems to be supported with Network APM must be certified by Verizon.
 - 1.2.2 **Network APM – Application Monitoring.** Verizon will monitor Customer's applications via application process/component run-time topology and process monitoring. Application topology maps the relationships of application components by process or function across a single host or multiple hosts. In addition, these components are monitored for availability and performance when applicable. A prerequisite for this feature option is Network APM – Server.
 - 1.2.3 **Network APM – End User Experience Monitoring.** This feature option uses end-to-end synthetic test agents to simulate user experience targeting specific applications. End-to-end agents measure and report back application performance perception scores at particular locations, so that Customer and Verizon can determine how the applications are performing for users at such locations as well as what the likely causes of any performance degradations.

1.2.3.1 **Nodes.** To collect the data from Managed Devices, Customer Equipment and/or other systems on the Customer Network, Network APM – End User Experience Monitoring utilizes agents to conduct synthetic tests on Customer applications (Nodes). All data collected by Nodes is fed into the Verizon Enterprise Center (VEC) platform in near real-time. The type of Nodes which may be employed with Network APM – End User Experience Monitoring include:

- **Enterprise Nodes:** Agents which are available in a variety of formats as virtual machines, containers, bare-metal which may be deployed into Customer’s data centers, offices, or into Infrastructure as a Service (IaaS).
- **Endpoint Nodes:** Agents which may be installed on a user device to gather user performance data either as real user monitoring or synthetic service, including Wi-Fi, LAN and network to the application from wherever the user is at the point in time.
- **Cloud Nodes:** Pre-implemented and managed by provider, these agents are used to execute Customer-defined tests from locations where Network APM – End User Experience Monitoring is available.
- **Backbone Nodes:** These agents measure digital services externally from datacenter-neutral facilities on various providers.
- **Last Mile Nodes:** These agents measure from real end user Internet Service Providers (ISPs). Last mile nodes are measured from end user ISPs and are hosted on dedicated devices in major locations.
- **Wireless Nodes:** These agents allow synthetic tests to be run on mobile end-user devices across various cellular networks around the world.

1.2.4 **Implementation Options.** Network APM offers two implementation options to bring devices under Verizon management: Managed Implementation and Managed Take Over. With Managed Implementation, Verizon provides support for the planning, system engineering, and overall project management of a new network. With Managed Takeover, Verizon reviews, optimizes, and takes over management of an existing Customer Network. Both implementation options are subject to a Statement of Requirements (SOR) to be agreed upon by the Parties. Both implementation options may not be available for every Network APM feature. Implementation options are available for each feature as indicated below:

Feature	Managed Implementation	Managed Take Over
Network APM-Server		✓
Network APM-Application Monitoring	✓	✓
Network APM-End User Experience Monitoring	✓	

1.2.4.1 **Due Diligence.** As a part of its due diligence during a Managed Take Over, Verizon will collect and analyze the logical and physical characteristics of Customer’s existing systems, as well as its related equipment or assets. All system data must be provided by Customer, including, but not limited to, Customer interviews, Customer-provided diagrams, and Customer Site-specific information.

1.2.4.2 **Impact Assessment.** For Managed Implementation or Managed Take Over, the Statement of Requirements is produced by Verizon in cooperation with Customer. The SOR (i) provides the inventory of the Customer Network, devices and/or current systems as it relates to the engagement of Network APM; (ii) identifies any physical/logical activities required to bring those devices, systems and Customer Network components under monitoring and/or management by Verizon, and (iii) identifies any gaps associated with facilitating the remote monitoring of the system components.

1.2.4.3 **Network Discovery.** Customer will provide Verizon with accurate information about proper scope of the Network Discovery, represents that it has all necessary authority to have

Verizon undertake the Network Discovery requested under these terms, and will indemnify Verizon and its employees, affiliates and agents against any liability if it does not. Verizon reserves the right to stop or withhold from performing Network Discovery, at its sole discretion. Customer's sole remedy for any failure, inadequacy or other problem of Network Discovery is to request that Verizon re-perform it. Network Discovery is provided as part of the Managed Take Over implementation. Otherwise, Customer may order Network Discovery for an additional Charge. If Customer orders Network Discovery, Verizon will electronically collect information on devices, hardware and systems that are connected to the Customer Network.

1.2.5 **Management Levels.** The availability of the management levels for each Network APM feature option is listed in the chart below.

	Monitor and Notify	Full
Network APM-Server	✓	✓
Network APM-Application Monitoring	✓	
Network APM-End User Experience Monitoring	✓	✓

1.2.5.1 **Network APM Monitor and Notify.** Network APM Monitor and Notify is available for all features under Network APM and provides the following:

- **Monitoring.** Verizon monitors features 24 hours a day, 7 days a week, using simple network management protocol (SNMP), internet control message protocol (ICMP – commonly referred to as a ping), and sometimes Windows Management Interface (WMI) for status and error conditions (e.g., SNMP trap messages or SNMP-based queries to operational state-of-target Managed Devices).
- **Notification.** Verizon will create a trouble ticket and attempt to notify Customer's designated point of contact within 15 minutes of Verizon's determination of a feature failure. Once the non-Verizon issue has been resolved by Customer, Verizon will close the ticket.
- **Reporting.** Upon Customer's order, Verizon will work with Customer to define the reporting views it requires for the applications monitored by Verizon. Selected reporting views will be made available via the VEC. Select reporting views will be made available via the VEC. All copies of reports, recommendations documentation VEC printouts, or other materials in any media form provided to Customer by Verizon are Verizon Confidential Information. Customer Confidential Information, if embedded in the reporting, shall continue to be treated as Customer Confidential Information.
- **Verizon Enterprise Center.** Verizon will provide Customer access to the Verizon Enterprise Center (VEC), a secure, scalable, consolidated view of Customer Network information, 24 hours a day, 7 days a week. The VEC provides access to project status, contact information, and information about Network APM. The VEC can be accessed at: <https://sso.verizonenterprise.com/amserver/sso/login.go?> Customer may have a maximum of 10 user accounts.
- **Network APM- End User Experience Monitoring Only.** For Monitor and Notify for Network APM- End User Experience Monitoring, Verizon does not create a trouble ticket for the Customer. Customer is responsible for resolving all faults.

1.2.5.2 **Full Management for Network APM - Server.** Full Management is available for Network APM-Server and provides the following, in addition to Monitor and Notify:

- For Network APM-Server-Hardware, Verizon identifies logical or physical issues with Customer's server hardware (with Customer's cooperation) whether the issue arose due to actions by Verizon, Customer or third parties. If the problem is hardware-related, Verizon Operations will notify Customer and affected third parties to remediate.

- For Network APM-Server-Operating System, Verizon identifies logical issues with Customer's Server Operating Systems (with Customer's cooperation) whether the issue arose due to actions by Verizon, Customer or third parties. Verizon will perform remote patch management on either Windows or Linux Operating Systems at Customer's direction and pursuant to Customer's IT policies.

1.2.5.3 **Full Management for Network APM-End User Experience Monitoring.** Full Management is available for Network APM-End User Experience Monitoring and provides the following, in addition to what is provided for Monitor and Notify for Network APM-End User Experience Monitoring. When Network APM-End User Experience Monitoring detects a fault, Verizon will create a trouble ticket and notify the Customer. The Verizon Network Operations Center will support the Customer in helping to work toward resolution of the fault.

1.3 **Customer Responsibilities**

1.3.1 **Change Management.** Except for Full Management, Customer will manage changes to the Customer Network and any routine maintenance of Managed Devices. Customer will also inform Verizon of any changes to the Customer Network that affect monitoring of the Customer Network including, but not limited to, removing managed components (such as a physical server, operating system, or data within an application, e.g., a database) from service.

1.3.2 **Provision of Managed Devices.** Verizon may require Customer to upgrade Managed Devices to meet the standards required by Verizon to provide Network APM. To facilitate data collection methods for monitoring, Customer will provide user authentication into its enterprise directory services, e.g., Active Directory or LDAP. In such cases, Network APM does not include the administration of such enterprise directory services.

1.3.3 **Software License Obligations.** If Customer selects a feature of Network APM that requires a Software License, Customer will comply and require its end users to comply, with all obligations set forth in any applicable end user software licenses.

1.3.4 **Customer Notifications.** Customer will report detected service failures and provide information to the Verizon Customer Service Center.

1.3.5 **Back Up.** Customer is responsible for the adequacy of any duplication or documentation for its electronic files at all times. Neither Verizon nor its designees are responsible or liable for data or files lost during the performance of Network APM.

1.3.6 **Physical Verification of Managed Devices.** Upon Verizon's request, Customer will reboot the Managed Devices, provide the LED light statuses of the Systems, provide the LED light statuses of the third party telecommunications provider network terminating unit (Telco NTU) where applicable, verify equipment power, verify if all cables are securely connected, and insert a loopback plug.

1.3.7 **Customer-Initiated Site Maintenance.** Customer will notify Verizon via a Customer Maintenance Change Management Request of any maintenance (powering down the site/managed device/managed system/Telco NTU, resetting equipment, re-cabling, physical equipment move) that may affect the operating status of the Managed Devices. Customer will notify Verizon of any system-, operating system-, or application-related changes that affect the topology dependencies.

1.3.8 **Customer Responsibilities for Monitor and Notify Service.** Customer will resolve both logical and physical faults, and fault isolation and associated downstream attached components (e.g., cabling, servers, non-managed switches, firewalls, and personal computers). Customer is responsible for the management of all equipment connected to managed components that are out of the scope of Network APM and for software licenses

associated with managed components. Customer will provide to Verizon the SNMP read access community string and WMI authentication for all Managed Devices.

- 1.3.9 **Customer Responsibilities under Full Management.** For Network APM-Server and Network APM-End User Experience Monitoring, Customer will facilitate the execution of a Letter of Authority (LOA) allowing Verizon to work with any third party maintenance providers. For Network APM – Server for operating systems, Customer will be responsible for providing Verizon with patch updates and identifying which target systems must be updated.

2. SUPPLEMENTAL TERMS

2.1 Country Related Limitations

- 2.1.1 **EMEA.** Verizon may, by virtue of providing Network APM-End User Experience Monitoring to Customer in the European Union, come into possession of Customer Data in connection with the provision of Network APM-End User Experience Monitoring. Verizon will act as Data Processor, as defined in the EU Data Protection Directive 95/46 (the Directive), on behalf of the Customer in providing Network APM-End User Experience Monitoring. Verizon will act as “Data Processor,” as defined in the EU Data Protection Directive 95/46 (the Directive), on behalf of the Customer in providing Network APM-End User Experience Monitoring. Verizon will implement appropriate technical and organizational measures to protect Customer Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against other unlawful forms of processing. Customer warrants that in its responsibility as “Data Controller” as defined and pursuant to the provisions of the Directive, it has obtained and will obtain all legally required consents and permissions from relevant parties (including, but not limited to, Customer’s end users as applicable) for the use, processing, and transfer of Customer Data as described in this section. Customer warrants that it has obtained and will obtain all legally required consents and permissions from relevant parties (including, but not limited to, Customer’s end users as applicable) for the use, processing and transfer of Customer Data pursuant to the provision of Network APM-End User Experience Monitoring.
- 2.1.2 **U.S.** If Customer chooses to use Network APM in the U.S., Customer will be considered a Data Controller as that term is used in the Data Protection Act 1998 and the Privacy and Electronic Communications Regulation 2003, and Customer is subject to all obligations applying to a data controller under those laws and other applicable laws and regulations. Verizon, while processing any resulting data on behalf of Customer, disclaims all responsibility for the decision to activate the feature, the manner in which such data is used by Customer, and the obtaining of Customer’s end users’ consent. Verizon will not process such data for any purpose other than to provide Network APM to Customer.

- 2.2 **Customer Data.** Verizon may collect information from during registration, or through communications by phone, e-mail, or otherwise from employees, contractors or other persons who use Customer’s Network APM, (Authorized Users). Verizon also collects measurement data, which includes the IP address of the applicable Managed Device and the IP address used to connect the Managed Device to networks, applications, and services. The measurement data is analyzed to provide Customer with information regarding the digital performance of its products and/or services including, but not limited to, the results generated by Network APM (Content). When Authorized Users access the Content, Verizon may automatically collect technical data including login information, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform. All the foregoing will be included in the definition of Customer Data. Customer agrees that it will not use Network APM with applications that collect or store personally identifiable information or with applications that must comply with any data privacy regulations including, but not limited to, the Payment Card Industry-Data Security Standards (PCI-DSS), Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), CA SB1386, the Federal Information

Security Management Act (FISMA) or the General Data Protection Regulation (GDPR). Customer is responsible for limiting or restricting the collection of sensitive data by Network APM.

2.3 **License Grant.** Verizon hereby grants to Customer, and Customer hereby accepts, a non-exclusive, non-transferable, revocable license to access and use Network APM solely for Customer's internal business purposes (the License). Verizon will provide Customer with proprietary software and documentation, including third party software and certain open source software (OSS)¹ (collectively, the Software) to enable Customer's use of Network APM in accordance with the License. Customer may authorize an unlimited number of its employees and contractors to use Network APM pursuant to the License, provided that, Customer shall be responsible for ensuring that all Authorized Users abide by the License and the terms set forth in Sections 2.3 through 2.5 (Required Terms). Pursuant to the License and specific user privileges granted by Verizon, Customer and its Authorized Users are permitted to view, print and/or download the Content solely for Customer's internal business purposes. No part of the Content is intended to constitute advice and should not be relied upon when making any decisions or taking any action of any kind. In order to access and use Network APM, the Managed Device used by Authorized Users must meet the certain specifications as required by Verizon. Verizon reserves the right to suspend, withdraw, discontinue or change all or any part of Network APM without notice or liability.

2.4 **License Restrictions.** Except as expressly permitted by the License, applicable OSS licenses, or local law, Customer shall not (and shall ensure that its Authorized Users and third parties do not):

- copy, modify, adapt, merge, combine, alter, enhance, translate, or create derivative works of, Network APM or the Software (or any part thereof), or permit others to do so;
- disassemble, decompile, reverse engineer or otherwise attempt to derive or access the source code of any proprietary software used by Verizon and/or its provider to provide Network APM, or permit others to do so;
- remove, alter or destroy any proprietary markings, copyright notices, confidential legends or any trademarks or trade names of Verizon or its providers placed upon or contained within Network APM and/or the Software;

¹The license grant to OSS is pursuant to the following licenses:

Cryptographic software libraries:

- OpenSSL (<http://www.openssl.org>) to ensure secure communications with the Analytics Cloud.
- PyCrypto (<http://www.pycrypto.org>) to encrypt configuration information locally on the device on which the Digital User is installed.

Open-source software libraries:

- Python 2.7, licensed under the Python Software Foundation License Version 2 (<https://www.python.org>)
- pywin32, licensed under the Python Software Foundation License (<https://sourceforge.net/projects/pywin32/>)
- TkInter, licensed under the Python Software Foundation license (<http://tkinter.unpythonic.net/wiki/Tkinter>)
- beautifulsoup4, licensed under the MIT license (<http://www.crummy.com/software/BeautifulSoup/>)
- html5lib, licensed under the MIT license (<https://pypi.python.org/pypi/html5lib>)
- six, licensed under the MIT license (<https://pypi.python.org/pypi/six/1.10.0>)
- psutil, licensed under the BSD3 license (<http://psutil.googlecode.com>)
- lxml, licensed under the BSD3 license (<http://lxml.de/>)
- Tcl/Tk 8.5, license based on the BSD license (<https://www.tcl.tk/software/tcltk/license.html>)
- curl, licensed under the MIT/X license (<http://curl.haxx.se>)
- pyCurl, licensed under the MIT/X license (<https://github.com/pycurl/pycurl>)
- sqlite3, in the public domain (<https://sqlite.org/>)
- pacparser, licensed under the LGPL3.0 license (<http://code.google.com/p/pacparser>)
- cx_freeze, licensed derived from the Python Software Foundation License (https://anthony-tuininga.github.io/cx_Freeze/)
- cx_logging, specific license (<http://cx-logging.sourceforge.net/LICENSE.txt>)

- fail to properly supervise and control use of Network APM and/or the Software;
- sublicense, sell, resell, rent, lease, transfer, timeshare, assign, distribute, display or disclose to any third party, commercially exploit Network APM and/or the Software (including operating as a service bureau or providing access to Network APM and/or the Software as an application service provider), or otherwise make Network APM and/or the Software (or any part thereof) available to any third party;
- use the Software in violation of any applicable laws and regulations (including without limitation any export laws, restrictions, national security controls and regulations); or
- cause the decompiling, disassembly, or reverse engineering of any portion of the Software, or attempt to discover any source code or other operational mechanisms of the Software.

Customer shall not (and shall ensure that its Authorized Users and third parties do not) use Network APM:

- to gather, extract, download, reproduce, use and/or display any information, content, material or data, whether by use of automated programs, robots, web crawlers, spiders, data mining, trawling or other "screen scraping" software or systems without Customer's prior written consent; or
- to damage, interfere with or disrupt access to Network APM, or do anything which may interrupt or impair their functionality, including, without limitation, by uploading or otherwise distributing files that contain viruses, corrupted files, Trojan horses, or any other similar software or programs that may be used to access, modify, delete or damage any data files or other computer programs used by Verizon or other users of Network APM.

2.5 **Authorized User Registration.** Authorized Users may complete a registration process which includes the creation of a user identifier and/or password. Authorized Users are solely responsible for ensuring that their user identifiers and passwords are kept confidential, and shall not disclose to, or allow user identifiers and/or passwords to be used by, any third party. In the event that Customer or any Authorized User has reason to believe that any user identifier and/or password is no longer secret, they will notify Verizon immediately. Customer reserves the right to disable any user identification code or password at any time without notice if an Authorized User fails to comply with the Required Terms.

2.6 **Disclaimer.** Verizon makes no warranties, guarantees, or representations, express, or implied that (a) Network APM will protect the Customer Network from intrusions, viruses, Trojan horses, worms, time bombs, cancel bots or other similar harmful or destructive programming routines; (b) any security threats and vulnerabilities will be prevented or detected; or (c) the performance by Verizon of Network APM will render Customer's systems invulnerable to security breaches.

3. **SERVICE LEVEL AGREEMENT.** The SLA for Network APM may be found by clicking on the following: www.verizon.com/business/service_guide/reg/cp_napm_sla.pdf.

4. **FINANCIAL TERMS.** Customer will pay charges for Network APM specified in the Agreement, including those below and at the following URL: www.verizon.com/business/service_guide/reg/applicable_charges_toc.htm. Charges below are in U.S. dollars and will be billed in the invoice currency of the associated service.

4.1 **Administrative Charges**

Administrative Charge	Charge Instance	NRC
Expedite Fee	Upon Customer Request	\$1,100.00
After Hours: Installation	Per site	\$600.00

4.2 **Optional Change Management.** Customer will pay the charges below for Optional Change

Management (OCM), which are not covered by the Standard Change Management activities shown in the VEC and included in the MRCs for Network APM.

Network APM OCM Charges		
Change	Change Instance (Charged per Server or Operating System unless noted)	NRC
After Hours: Changes	Per request per site	\$600.00
Implementation (Modify Existing)	Change per Server or Operating System	\$50.00
Design (Single Feature/Protocol)	Change per Server or Operating System	\$250.00
Design Plus (Multiple Feature/Protocol)	Change per Server or Operating System	\$400.00

4.3 **IP Addresses.** Verizon may use secondary IP addressing if Customer is using unregistered IP address space. If Customer does not allow secondary IP addressing, Customer will pay reasonable costs for a dedicated management domain or an IP proxy hardware solution.

5. **DEFINITIONS.** The following definitions apply to Network APM, in addition to those identified in the Master Terms and the administrative charge definitions at the following URL:
www.verizon.com/business/service_guide/reg/definitions_toc_2017DEC01.htm.

Term	Definition
After Hours	Outside of the hours between 9:00am and 5:00pm on a Business Day in the time zone of the Customer Site receiving Network APM.
Customer Network	A collection of Managed Devices and the network they are connected to.
Managed Devices	Items of CPE that have been designated as supported by Network APM.