

**AppNeta**

Customizable Runbook Templates

**User Guide**

**Version 2.1 (document)**

Copyright © 2024 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, go to [www.broadcom.com](http://www.broadcom.com). All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

**Table of Contents**

[Chapter 1: Overview 4](#_Toc162972551)

[Template Instructions 4](#_Toc162972552)

[Primary Contacts 4](#_Toc162972553)

[Technical Support 4](#_Toc162972554)

[AppNeta Login Instructions 5](#_Toc162972555)

[User Management 5](#_Toc162972556)

[Use Case Overview 6](#_Toc162972557)

[Deployment Overview 6](#_Toc162972558)

[Integrations 6](#_Toc162972559)

[Terminology 6](#_Toc162972560)

[Chapter 2: Deploy a New Monitoring Point 8](#_Toc162972561)

[Deploy new Windows Native Monitoring Points 8](#_Toc162972562)

[Deploy new Mac Native Monitoring Points 8](#_Toc162972563)

[Deploy new m70 Monitoring Points 9](#_Toc162972564)

[Deploy new r90 Monitoring Points 9](#_Toc162972565)

[Deploy new r1000 Monitoring Points 9](#_Toc162972566)

[Deploy new CMP in AWS 10](#_Toc162972567)

[Deploy new CMP in Azure 10](#_Toc162972568)

[Deploy new CMP in GCP 10](#_Toc162972569)

[Deploy new cpe40 on a Cisco Switch 11](#_Toc162972570)

[Deploy new cpe40 on an Arista Switch 11](#_Toc162972571)

[Deploy new v35 on a KVM Hypervisor 11](#_Toc162972572)

[Deploy new v35 on a VMware Hypervisor 12](#_Toc162972573)

[Chapter 3: Configure Network Monitoring 13](#_Toc162972574)

[Monitor a new Application or Network Target 13](#_Toc162972575)

[Monitor from a new Monitoring Point 13](#_Toc162972576)

[Chapter 4: Configure Web App Monitoring 14](#_Toc162972577)

[Monitor a new Application 14](#_Toc162972578)

[Monitor from a new Monitoring Point 14](#_Toc162972579)

[Chapter 5: Configure Usage Monitoring 15](#_Toc162972580)

[Monitor from a new Monitoring Point 15](#_Toc162972581)

[Chapter 6: Network Monitoring Alert Runbooks 16](#_Toc162972582)

[Connectivity Loss (Network Path) 16](#_Toc162972583)

[Data Jitter 16](#_Toc162972584)

[Data Loss 17](#_Toc162972585)

[Latency 18](#_Toc162972586)

[MOS (Mean Opinion Score) 19](#_Toc162972587)

[QoS Change 19](#_Toc162972588)

[Round Trip Time (RTT) 20](#_Toc162972589)

[Voice Jitter 21](#_Toc162972590)

[Voice Loss 21](#_Toc162972591)

[Chapter 7: Web App Monitoring Alert Runbooks 23](#_Toc162972592)

[Apdex Score Violation 23](#_Toc162972593)

[Connectivity Loss (Web Path) 23](#_Toc162972594)

[HTTP Errors 24](#_Toc162972595)

[HTTP Status Violation 25](#_Toc162972596)

[Page Load Time Violation 26](#_Toc162972597)

[Script Errors 26](#_Toc162972598)

[Transaction Time Violation 27](#_Toc162972599)

[Template Revision History 29](#_Toc162972600)

# Overview

**NOTE** For complete product documentation, visit [techdocs.broadcom.com/appneta](https://techdocs.broadcom.com/appneta).

## Template Instructions

1. Review this document and replace any instructions or placeholder text with information specific to your organization.
   1. Placeholder values are formatted as *<string>* throughout the template. For example, in alert runbooks, <n> is a placeholder for an integer.
2. Review alert playbooks and indicate any actions or investigation steps to be taken that are specific to your organization.
3. Remove sections not relevant to your AppNeta deployment (for example, remove Monitoring Point deployment playbooks for unused models, or remove alert playbooks for unused alert types).
4. To update the Table of Contents after making changes that affect the table of contents:
   1. In Google Docs, hover over the table of contents, then click **Update table of contents**.
   2. In Microsoft Word, right-click the table of contents, then select **Update field**.
5. Send feedback about this template to [appneta.education.pdl@broadcom.com](mailto:appneta.education.pdl@broadcom.com).

## Primary Contacts

*This section is intended to record key contacts and teams responsible for maintaining various aspects of the AppNeta deployment, such as infrastructure, installation, monitoring configuration, integrations, and so on.*

* *<Name>, <Email>, <Role or description of responsibility>*
* *<Name>, <Email>, <Role or description of responsibility>*
* *<Name>, <Email>, <Role or description of responsibility>*

## Technical Support

**​**Broadcom Support Portal: <https://support.broadcom.com>

A Broadcom Cloud user account is required to access the Broadcom Support Portal. The user account must have a Site ID associated with an AppNeta entitlement.

* Register for a new Broadcom Cloud user account at <https://profile.broadcom.com/web/registration>.
* To learn how to update a Broadcom Cloud user with a Broadcom Software Site ID, refer to the knowledge base article: [Using your Broadcom Site ID(s) for full support portal access](https://knowledge.broadcom.com/external/article/142873/manage-broadcom-site-ids-or-upgrade-your.html).

|  |  |
| --- | --- |
| **Support Site ID** | **Notes** |
|  |  |
|  |  |

## AppNeta Login Instructions

*This section is intended to record an instruction for how users should log in to AppNeta. For example,* ***Log in to AppNeta with <credentials> at <URL>****, where:*

* *<credentials> is the type of user credentials, for example,* your Broadcom Cloud account *or* your corporate credentials
* *<URL> is the login url, such as* <https://signon.pm.appneta.com/>*, or a custom url*

## User Management

*This section is intended to summarize how users are granted access to AppNeta. For example, the section could include details about a Single Sign-on (SSO) integration, whether users request access to AppNeta through an internal procedure, whether there is a request or approval process before access is granted, how user roles are assigned, and so on.*

### User Provisioning in AppNeta

*This section is intended to document how users are created within the AppNeta application.*

**For AppNeta SaaS:** Users created within the AppNeta user interface are tied to a Broadcom Cloud user account. Once a user is added to AppNeta, they may then use their Broadcom Cloud account to access AppNeta, the Broadcom Support portal, and any other Broadcom Cloud applications they are entitled to.

**For AppNeta On-Prem:** Users created within AppNeta remain separate from all other Broadcom applications and are managed entirely within AppNeta On-Prem.

### Single Sign-On (SSO)

*This section is intended to document how SSO was deployed, if applicable. For example:*

Broadcom Okta was integrated with *<Identity Provider>* on *<Date>* by *<Name>*.

SSO was enabled for AppNeta on *<Date>* by *<Name>*.

#### SSO Role Mapping

|  |  |
| --- | --- |
| **Security Group** | **AppNeta User Role** |
|  |  |
|  |  |

## Use Case Overview

*This section is intended to briefly summarize your organization’s primary monitoring goals for AppNeta.*

## Deployment Overview

*This section is intended for an overview of the AppNeta environment. Consider documenting where AppNeta is deployed, what is monitored, and the overall deployment strategy. Include diagrams of deployment and monitoring if available.*

## Integrations

*This section is intended for documentation about any integrations configured for AppNeta. As an example, a template for an integration with DX NetOps is included.*

### DX NetOps Integration

DX NetOps pulls AppNeta Monitoring Point and network monitoring data into DX NetOps Portal using the AppNeta integration and AppNeta API. AppNeta is configured to send notifications about events to DX NetOps Spectrum OneClick.

**DX NetOps integration contact:** *<Name>*, *<Email or other contact method>*

**AppNeta Access Token expiration date:** *<Date>*

*<Note describing how token management will be handled>*

#### VNA Plugin Configuration:

* **Plugin Name:** AppNeta Plugin
* **APPNETA\_HOST:** *<example.pm.appneta.com>*

#### AppNeta SNMP Notification Configuration:

* **Primary Trap Sender:** *<Monitoring Point Name>*
* **NMS Host(s):** *<SpectroSERVER IP address>*
* **Port:** *<SpectroSERVER port number>*
* **SNMP Version**: <*v2c* OR *v3*>
* **Delivery Type**: trap
* **Trap Community**: *<SpectroSERVER SNMP community string>*

## Terminology

* **Delivery:** The Delivery area of the AppNeta user interface provides network performance monitoring.
  + **Single-ended monitoring:** Network monitoring performed from a Monitoring Point to any target measuring round trip performance, primarily using ICMP.
  + **Dual-ended monitoring:** Network monitoring performed between two Monitoring Points, measuring upload and download performance independently, primarily using UDP.
  + **Network path:** The object created in AppNeta to represent continuous network monitoring performed from an individual Monitoring Point to an individual target.
* **Experience:** The Experience area of the AppNeta user interface provides web application monitoring.
* **Usage:** The Usage area of the AppNeta user interface provides passive traffic monitoring, application identification, and packet capture capabilities.
* **Monitoring Point:** Generic term for any hardware, software or virtual installation performing monitoring as part of an AppNeta account.
  + **Physical Monitoring Point:** A Monitoring Point deployed via AppNeta hardware appliance.
  + **Native Monitoring Point (NMP):** A Monitoring Point deployed via AppNeta software installed on a supported Mac or Windows machine.
  + **Container-based Monitoring Point (CMP):** A Monitoring Point running on a Docker container.
  + **Customer Premise Equipment (CPE):** Monitoring Point running on a Docker container deployed on supported hardware, such as a Cisco Catalyst 9300/9400 switch.
  + **Virtual Monitoring Point (v35):** A Monitoring Point deployed as a virtual machine on VMware or KVM.
  + **Global Monitoring Point (GMP):** Cloud-based installations managed by AppNeta (but owned by an individual customer) for performing Experience and Delivery monitoring.
  + **Global Monitoring Target (GMT):** Cloud-based installations managed by AppNeta for customers to use as highly available targets for monitoring internet connectivity.

# Deploy a New Monitoring Point

**NOTE ​​**Once a Monitoring Point is installed, some customization steps are necessary to complete the deployment and commence monitoring.

## Deploy new Windows Native Monitoring Points

**NOTE** See AppNeta documentation for [host requirements](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/windows-mp-intro/windows-specifications1/windows-mp-port-descriptions.html), [set up prerequisites and detailed installation instructions](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/windows-mp-intro/windows-setup/windows-mp-setup-nmp-windows.html), and [Windows firewall rules](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-firewall.html#firewall-configuration_configuring-for-an-nmp-on-windows).

### Unattended Installation for Windows

1. Navigate to *<configuration management tool repository>* and select the appropriate AppNeta installer.
   * See installation instructions for steps to download the Windows (native) installation package from AppNeta.
2. Deploy this image to all relevant workstations.
3. Check the [Monitoring Points page](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to confirm new Monitoring Points connected to AppNeta.
   * [Troubleshoot connectivity to AppNeta](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/windows-mp-intro/windows-setup/windows-mp-troubleshooting-connectivity-to-appneta.html)
4. Optionally, [assign relevant custom tags](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to Monitoring Points. Once you have monitoring policies configured, assigning tags to Monitoring Points may automatically start monitoring according to existing monitoring policy rules.
5. Configure additional network monitoring (see Chapter 3), and HTTP monitoring (see Chapter 4) as required.

### Manual Installation for Windows

Refer to the [manual install instructions](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/windows-mp-intro/windows-setup/windows-mp-setup-nmp-windows.html#mp-setup-nmp-windows_manual-install) in AppNeta documentation (instructions are available for download in .DOCX and .PDF format).

## Deploy new Mac Native Monitoring Points

**NOTE** See AppNeta documentation for [host requirements](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/macos-mp-intro/macos-specifications1/macos-mp-port-descriptions.html), [set up prerequisites, and detailed installation instructions](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/macos-mp-intro/macos-setup/macos-mp-setup-nmp-macos.html).

### Unattended Installation for macOS

1. Navigate to *<configuration management tool repository>* and select the appropriate AppNeta Installer.
   * See installation instructions for steps to download the macOS (native) installation package from AppNeta.
2. Deploy this image to all relevant workstations.
3. Check the [Monitoring Points page](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to confirm new Monitoring Points connected to AppNeta
   * [Troubleshoot connectivity to AppNeta](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/macos-mp-intro/macos-setup/macos-mp-troubleshooting-connectivity-to-appneta.html).
4. Optionally, [assign relevant custom tags](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to Monitoring Points. Once you have monitoring policies configured, assigning tags to Monitoring Points may automatically start monitoring according to existing monitoring policy rules.
5. Configure additional network monitoring (see Chapter 3), and HTTP monitoring (see Chapter 4) as required.

### Manual Installation for macOS

Refer to the [manual install instructions](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/macos-mp-intro/macos-setup/macos-mp-setup-nmp-macos.html#mp-setup-nmp-macos_manual-install1) in AppNeta documentation (instructions are available for download in .DOCX and .PDF format).

## Deploy new m70 Monitoring Points

1. Connect Monitoring Point to your network (see [m70 Setup Guide PDF](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/m70-mp-intro/m70-setup/m70-mp-setup-guide-pdf.html)).
   * Review and connect optional connections.
2. Check the [Monitoring Points page](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to confirm new Monitoring Points connected to AppNeta.
   * [Troubleshoot connectivity to AppNeta](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/m70-mp-intro/m70-setup/m70-mp-troubleshooting-connectivity-to-appneta.html).
3. Configure a [wireless interface](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/m70-mp-intro/m70-configuration/m70-mp-wireless-interfaces.html) (you will need the SSID, the security type, and the passphrase for the wireless network).
4. Optionally, add [additional interfaces](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/m70-mp-intro/m70-setup/m70-mp-setup-physical.html#mp-setup-physical_mp-phys-config-additional-features) (for example, VLAN tagged interfaces).
5. Optionally, [assign relevant custom tags](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to automatically start monitoring according to existing monitoring policy rules.
6. Configure additional network monitoring (see Chapter 3), web app monitoring (see Chapter 4), and usage monitoring (see Chapter 5) as required.

## Deploy new r90 Monitoring Points

1. Connect Monitoring Point to your network (see [r90 Setup Guide PDF](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/r90-mp-intro/r90-setup/r90-mp-setup-guide-pdf.html))
   * Review and connect optional connections
2. Check the [Monitoring Points page](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to confirm new Monitoring Points connected to AppNeta
   * [Troubleshoot connectivity to AppNeta](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/r90-mp-intro/r90-setup/r90-mp-troubleshooting-connectivity-to-appneta.html)
3. Add [additional interfaces](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/r90-mp-intro/r90-setup/r90-mp-setup-physical.html#mp-setup-physical_mp-phys-config-additional-features) if needed (for example, VLAN tagged interfaces)
4. Optionally, [assign relevant custom tags](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to Monitoring Points. Once you have monitoring policies configured, assigning tags to Monitoring Points may automatically start monitoring according to existing monitoring policy rules.
5. Configure network monitoring (see Chapter 3), web app monitoring (see Chapter 4), and usage monitoring (see Chapter 5).

## Deploy new r1000 Monitoring Points

1. Connect Monitoring Point to your network (see [r1000 Setup Guide PDF](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/r1000-mp-intro/r1000-setup/r1000-mp-setup-guide-pdf.html)).
   * Review and connect optional connections.
2. Check the [Monitoring Points page](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to confirm new Monitoring Points connected to AppNeta.
   * [Troubleshoot connectivity to AppNeta](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/r1000-mp-intro/r1000-setup/r1000-mp-troubleshooting-connectivity-to-appneta.html).
3. Optionally, add [additional interfaces](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/r1000-mp-intro/r1000-setup/r1000-mp-setup-physical.html#mp-setup-physical_mp-phys-config-additional-features) (for example, VLAN tagged interfaces).
4. Optionally, [assign relevant custom tags](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to Monitoring Points. Once you have monitoring policies configured, assigning tags to Monitoring Points may automatically start monitoring according to existing monitoring policy rules.
5. Configure additional network monitoring (see Chapter 3), web app monitoring (see Chapter 4), and usage monitoring (see Chapter 5) as required.

## Deploy new CMP in AWS

**NOTE** See AppNeta documentation for [host requirements and prerequisites](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/aws-mp-intro/aws-specifications1/aws-mp-port-descriptions.html).

1. [Install the CMP](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/aws-mp-intro/aws-setup/aws-mp-setup-cmp.html) using Docker Compose.
2. Check the [Monitoring Points page](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to confirm new Monitoring Points connected to AppNeta.
   * [Troubleshoot connectivity to AppNeta](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/aws-mp-intro/aws-setup/aws-mp-troubleshooting-connectivity-to-appneta.html).
3. Optionally, [assign relevant custom tags](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to Monitoring Points. Once you have monitoring policies configured, assigning tags to Monitoring Points may automatically start monitoring according to existing monitoring policy rules.
4. Configure additional network monitoring (see Chapter 3), and web app monitoring (see Chapter 4) as required.

## Deploy new CMP in Azure

**NOTE** See AppNeta documentation for [host requirements](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/azure-mp-intro/azure-specifications1/azure-mp-port-descriptions.html), and [deployment options, prerequisites, and detailed installation instructions](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/azure-mp-intro/azure-setup/azure-mp-setup-cmp.html).

1. [Install the CMP](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/azure-mp-intro/azure-setup/azure-mp-setup-cmp.html) either using Azure Kubernetes Service (AKS) or using Docker Compose.
2. Check the [Monitoring Points page](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to confirm new Monitoring Points connected to AppNeta.
   * [Troubleshoot connectivity to AppNeta](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/azure-mp-intro/azure-setup/azure-mp-troubleshooting-connectivity-to-appneta.html).
3. Optionally, [assign relevant custom tags](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to Monitoring Points. Once you have monitoring policies configured, assigning tags to Monitoring Points may automatically start monitoring according to existing monitoring policy rules.
4. Configure additional network monitoring (see Chapter 3), and web app monitoring (see Chapter 4) as required.

## Deploy new CMP in GCP

**NOTE** See AppNeta documentation for [host requirements](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/gcp-mp-intro/gcp-specifications1/gcp-mp-port-descriptions.html), and [deployment options, prerequisites, and detailed installation instructions](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/gcp-mp-intro/gcp-setup/gcp-mp-setup-cmp.html).

1. [Install the CMP](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/gcp-mp-intro/gcp-setup/gcp-mp-setup-cmp.html) using Docker Compose.
2. Check the [Monitoring Points page](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to confirm new Monitoring Points connected to AppNeta.
   * [Troubleshoot connectivity to AppNeta](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/gcp-mp-intro/gcp-setup/gcp-mp-troubleshooting-connectivity-to-appneta.html).
3. Optionally, [assign relevant custom tags](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to Monitoring Points. Once you have monitoring policies configured, assigning tags to Monitoring Points may automatically start monitoring according to existing monitoring policy rules.
4. Configure additional network monitoring (see Chapter 3), and web app monitoring (see Chapter 4) as required.

## Deploy new cpe40 on a Cisco Switch

**NOTE** See AppNeta documentation for [host requirements](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/cisco-cpe40-mp-intro/cisco-cpe40-specifications1/cisco-cpe40-mp-port-descriptions.html) and [setup prerequisites](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/cisco-cpe40-mp-intro/cisco-cpe40-setup/cisco-cpe40-mp-setup-cpe.html).

1. Follow the documented [cpe40 setup instructions for Cisco](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/cisco-cpe40-mp-intro/cisco-cpe40-setup/cisco-cpe40-mp-setup-cpe.html) to:
   * Initiate the installation process
   * Enable the Application Hosting framework
   * Download the cpe40 image and checksum file
   * Install the cpe40
   * Configure application hosting
   * Activate the application
   * Start the application
   * Verify the Installation
   * Save the Configuration
2. Check the [Monitoring Points page](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to confirm new Monitoring Points connected to AppNeta.
   * [Troubleshoot connectivity to AppNeta](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/cisco-cpe40-mp-intro/cisco-cpe40-setup/cisco-cpe40-mp-troubleshooting-connectivity-to-appneta.html).
3. Optionally, [assign relevant custom tags](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to Monitoring Points. Once you have monitoring policies configured, assigning tags to Monitoring Points may automatically start monitoring according to existing monitoring policy rules.
4. Configure additional network monitoring (see Chapter 3), and HTTP monitoring (see Chapter 4) as required.

## Deploy new cpe40 on an Arista Switch

**NOTE** See AppNeta documentation for [host requirements](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/cisco-cpe40-mp-intro/cisco-cpe40-specifications1/cisco-cpe40-mp-port-descriptions.html) and [setup prerequisites](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/arista-cpe40-mp-intro/arista-cpe40-setup/arista-cpe40-mp-setup-cpe-arista.html).

1. Follow the documented [cpe40 setup instructions for Arista](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/arista-cpe40-mp-intro/arista-cpe40-setup/arista-cpe40-mp-setup-cpe-arista.html) to:
   * Initiate the installation process
   * Enable SCP
   * Install the Docker runtime extension
   * Enable container manager
   * Download the cpe40 image and checksum file
   * Install the cpe40
2. Check the [Monitoring Points page](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to confirm new Monitoring Points connected to AppNeta.
   * [Troubleshoot connectivity to AppNeta](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/arista-cpe40-mp-intro/arista-cpe40-setup/arista-cpe40-mp-troubleshooting-connectivity-to-appneta.html).
3. Optionally, [Assign relevant custom tags](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to Monitoring Points. Once you have monitoring policies configured, assigning tags to Monitoring Points may automatically start monitoring according to existing monitoring policy rules.
4. Configure additional network monitoring (see Chapter 3), and HTTP monitoring (see Chapter 4) as required.

## Deploy new v35 on a KVM Hypervisor

**NOTE** See AppNeta documentation for [setup prerequisites](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/v35-kvm-mp-intro/v35-kvm-setup/v35-kvm-mp-setup-v35-kvm.html) and [guest requirements](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/v35-kvm-mp-intro/v35-kvm-specifications1/v35-kvm-mp-guest-requirements.html). Review [additional features](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/v35-kvm-mp-intro/v35-kvm-setup/v35-kvm-mp-setup-v35-kvm.html#mp-setup-v35-kvm_configure-additional-features-if-required).

1. Follow the documented [setup instructions](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/v35-kvm-mp-intro/v35-kvm-setup/v35-kvm-mp-setup-v35-kvm.html) to:
   * Set up a KVM host
   * Load install scripts
   * Load base and config images
   * Create a v35 virtual machine
   * Configure for web proxy (if required)
2. Check the [Monitoring Points page](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to confirm new Monitoring Points connected to AppNeta.
   * [Troubleshoot connectivity to AppNeta](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/v35-kvm-mp-intro/v35-kvm-setup/v35-kvm-mp-troubleshooting-connectivity-to-appneta.html).
3. Optionally, [configure for Usage monitoring](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/v35-kvm-mp-intro/v35-kvm-setup/v35-kvm-mp-setup-v35-kvm.html#mp-setup-v35-kvm_set-up-v35-for-usage-monitoring).
4. [Change the default password](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/v35-kvm-mp-intro/v35-kvm-access/v35-kvm-mp-access-credentials.html#access-credentials_changing-monitoring-point-password).
5. Optionally, configure v35 for [additional required features](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/v35-kvm-mp-intro/v35-kvm-setup/v35-kvm-mp-setup-v35-kvm.html#mp-setup-v35-kvm_configure-additional-features-if-required) (for example, Usage monitoring, 10Gbps, VLAN).
6. Optionally, [assign relevant custom tags](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to Monitoring Points. Once you have monitoring policies configured, assigning tags to Monitoring Points may automatically start monitoring according to existing monitoring policy rules.
7. Configure additional network monitoring (see Chapter 3), web app monitoring (see Chapter 4), and usage monitoring (see Chapter 5) as required.

## Deploy new v35 on a VMware Hypervisor

**NOTE** See AppNeta documentation for [setup prerequisites](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/v35-vmware-mp-intro/v35-vmware-setup/v35-vmware-mp-setup-v35-vmware.html) and [guest requirements](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/v35-vmware-mp-intro/v35-vmware-specifications1/v35-vmware-mp-guest-requirements.html).

1. Follow the documented [setup instructions](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/v35-vmware-mp-intro/v35-vmware-setup/v35-vmware-mp-setup-v35-vmware.html) to:
   * Create a v35 virtual machine using vCenter or without using vCenter
   * Configure for web proxy (if required)
2. Check the [Monitoring Points page](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to confirm new Monitoring Points connected to AppNeta.
   * [Troubleshoot connectivity to AppNeta](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/v35-vmware-mp-intro/v35-vmware-setup/v35-vmware-mp-troubleshooting-connectivity-to-appneta.html).
3. Optionally [configure VMware for Usage monitoring](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/v35-vmware-mp-intro/v35-vmware-setup/v35-vmware-mp-setup-v35-vmware.html#mp-setup-v35-vmware_mp-configure-for-usage).
4. [Change the default password](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/appliance-overview/v35-vmware-mp-intro/v35-vmware-access/v35-vmware-mp-access-credentials.html#access-credentials_changing-monitoring-point-password).
5. Optionally, [assign relevant custom tags](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=mp-manage-all&appid=appneta&language=&format=rendered) to Monitoring Points. Once you have monitoring policies configured, assigning tags to Monitoring Points may automatically start monitoring according to existing monitoring policy rules.
6. Configure additional network monitoring (see Chapter 3), web app monitoring (see Chapter 4), and usage monitoring (see Chapter 5) as required.

# Configure Network Monitoring

Create monitoring policies in AppNeta to define which applications and network targets to monitor, and from which Monitoring Points.

**NOTE** You need an AppNeta user role of Organization Admin, Advanced, or Standard to configure monitoring policies.

## Monitor a new Application or Network Target

1. In AppNeta, select the appropriate organization from the user menu.
2. Navigate to **Settings cog collapsed**, then select **Monitoring Policies**.
3. Add a new monitoring policy for the application or network target.
   1. See [Manage Monitoring Policies](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=managing-monitoring-policies&appid=appneta&language=&format=rendered) for complete instructions.

**TIPS** Enter a friendly name for the target as the policy name. The friendly name is especially useful when the target is an anonymous IP address.  
  
Create dynamic Monitoring Point rules using custom tags to automatically start monitoring from new Monitoring Points that meet the specified criteria.  
  
To set up dual-ended monitoring, target another AppNeta Monitoring Point. In the policy, expand **Network Settings** and turn on dual-ended monitoring.

1. Click **Preview** to review the policy. Preview shows the impact of changes to a monitoring policy. Make sure to review the total number of paths to be created and deleted as a result of your configuration choices.
2. Click **Update** to create the policy.
   1. If the policy is enabled, monitoring begins from new Monitoring Points added to the policy and monitoring stops from Monitoring Points removed from the policy.
   2. If data deletion is turned on, historical monitoring data is immediately deleted when a Monitoring Point no longer matches the policy rules.
   3. If data deletion is turned off, historical data is maintained for the life of the policy, subject to the standard data retention period.

## Monitor from a new Monitoring Point

**NOTE** Monitoring will automatically start from new Monitoring Points that meet the rules defined in a monitoring policy. If monitoring does not begin as expected, check the Monitoring Point rules in the policy and whether the required custom Monitoring Point tags were applied to the new Monitoring Point.

# Configure Web App Monitoring

## Monitor a new Application

1. In AppNeta, choose the appropriate organization from the user menu at the top right of the page.
2. Create a new Web App Group including the source locations, the target URL, and either a Browser or HTTP workflow.
   1. See [Create a web app group](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=experience-web-app-groups&appid=appneta&language=&format=rendered) for step-by-step instructions.
   2. Use a Browser workflow to emulate users accessing a web app via a browser.
   3. Use an HTTP workflow to send HTTP requests to the web app’s API.
3. Click Save to apply the changes.

## Monitor from a new Monitoring Point

*​​In this section, it is recommended to add instructions for how to determine the appropriate Web App Group. For complex deployments, add a summary table defining all Web App Groups.*

1. In AppNeta, choose the appropriate organization from the user menu at the top right of the page.
2. Navigate to **Experience**, then **Web App Groups**.
3. Add new Monitoring Points to the appropriate Web App Groups.
   1. For the Web App Group you want to edit, click **Configure**.
   2. Click the **Monitor from** button.
   3. Search for the new source Monitoring Points.
4. Repeat for each new Monitoring Point.
   1. Click Save to apply the changes.

# Configure Usage Monitoring

## Monitor from a new Monitoring Point

**NOTE** [Review Usage prerequisites](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=usage-setup&appid=appneta&language=&format=rendered) and ensure Monitoring Point is properly cabled for Usage Monitoring.

1. In AppNeta, choose the appropriate organization from the user menu at the top right of the page.
2. [Define local subnets](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=usage-setup&appid=appneta&language=&format=rendered).
3. [Apply appropriate alert profile](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=usage-alerts&appid=appneta&language=&format=rendered), if applicable.
4. Apply relevant [custom application definitions](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=usage-custom-apps&appid=appneta&language=&format=rendered) as defined by your organization, if applicable.
5. [Start capturing traffic](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=usage-start-stop&appid=appneta&language=&format=rendered).

# Network Monitoring Alert Runbooks

These runbook templates cover how to handle an alert or notification triggered by Network Path violations.

## Connectivity Loss (Network Path)

* **Notification Type:** *<type, such as email or webhook>* sent to *<destination>*.
* **Threshold:** Alert triggered when a Monitoring Point does not receive a layer 2 response from the path target for *<n>* minutes.
* **Typical causes:** 
  + Infrastructure between the Monitoring Point and the target is down.
  + The target is down.
  + The target does not respond to ICMP (single-ended path) or UDP port 3239 (dual-ended path).
  + [A firewall](https://techdocs.broadcom.com/appneta-firewall) is not configured correctly for AppNeta.
* **Check whether other paths to the same target exhibit the same symptoms.**
  + Action: Filter to relevant paths and check the [Route Visualization](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-routes) to see where and when the break in connectivity occurred.
  + If only one or a small number of paths to the same target have lost connectivity, there is typically a network issue localized to the source location or region for those paths.
  + If all network paths from different source locations have lost connectivity to the same target, there is typically a problem at the target or its network infrastructure.

## Data Jitter

Jitter, also known as packet delay variation, is a measure of variation in latency. Jitter affects time-sensitive applications that use UDP but does not affect applications using TCP. Data jitter is measured when packet trains emulating data traffic are used for monitoring.

* **Notification Type:** *<type, such as email or webhook>* sent to *<destination>*.
* **Threshold**: Alerts when data jitter is greater than *<n>* milliseconds for *<n>* minutes.
* **Typical causes:** 
  + Network congestion
  + Lack of QoS configuration
  + Mis-configured QoS
  + Network devices changing QoS markings
* **Check:** [Network path performance charts](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=path-performance&appid=appneta&language=&format=rendered) for changes in Jitter and determine when they occurred. If needed, expand the timeline to include time leading up to alert.
  + Do any changes correlate with network changes made at the same time?
* **Check:** If test packets are [configured to use the same QoS markings](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=delivery-qos-templates&appid=appneta&language=&format=rendered) used by the traffic being emulated.
* **Review** [diagnostic tests](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-diagnostics) run during the violation event:
  + Check the QoS column on the [Data Details tab](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/network-performance-monitoring-delivery/delivery-results/delivery-diagnostics.html#title-diagnostics_data-and-voice-details-tabs). Make sure that the QoS markings are consistent (not being changed or dropped) along the path.
  + Check the Data Jitter and Latency columns on the [Data Details tab](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/network-performance-monitoring-delivery/delivery-results/delivery-diagnostics.html#title-diagnostics_data-and-voice-details-tabs). Look for significant jumps in Data Jitter or Latency along the path indicating a source of congestion.
  + Note that the cause of the unexpected jump in jitter can be at the first hop reporting the jump, the previous hop, or any infrastructure in between the two.
* **Check:** [Whether other paths to the same target exhibit the same symptoms](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_determine-the-scope-and-source-of-a-network-path-alert).
  + If only one or a small number of paths to the same target have the same violation, there is typically a network issue localized to the source location or region for those paths.
  + If many or all paths to the same target have the same violation, there is typically a problem at the target or its network infrastructure. Check the [Route Visualization](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-routes) to determine which network hops were common to all violating paths prior to and during the violation event.

## Data Loss

Packet loss, whether the packets are data or voice, is simply a measure of the number of packets that did not make it to their intended destination. Data loss is measured when packet trains emulating data traffic are used. (Read more about [Data Loss violations](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_data-loss).)

* **Notification Type:** *<type, such as email or webhook>* sent to *<destination>*.
* **Threshold:** Alerts when *<n>*% of data packets are lost in tests occurring for *<n>* minutes.
* **Typical causes:** 
  + Traffic congestion along the network path
  + An overloaded network device
  + Bad physical media
  + Flapping routes
  + Flapping load balancing
  + Name resolution issues
  + MTU mismatch
  + Firewall protecting against DDOS resulting in a loss plateau (e.g. exactly 50% loss)
  + Selected target does not respond well to test packets
* **Check:** [Network path performance charts](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=path-performance&appid=appneta&language=&format=rendered) for changes in Data Loss and determine when they occurred. If needed, expand the timeline to include time leading up to alert.
  + Do any changes in Data Loss correlate with network changes made at the same time?
  + If you see a jump in Data Loss but no Voice Loss this is highly indicative of a problem with MTU.
* **Review** [diagnostic tests](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-diagnostics) run during the violation event. Check the Data Loss column on the [Data Details tab](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/network-performance-monitoring-delivery/delivery-results/delivery-diagnostics.html#title-diagnostics_data-and-voice-details-tabs). Look for a hop reporting non-zero data loss that continues to be reported at all subsequent hops along the route.
  + Note that the cause of data loss can be at the first hop reporting data loss, the previous hop, or any infrastructure in between the two.
* **Check:** [Whether other paths to the same target exhibit the same symptoms](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_determine-the-scope-and-source-of-a-network-path-alert).
  + If only one or a small number of paths to the same target have the same violation, there is typically a network issue localized to the source location or region for those paths.
  + If many or all paths to the same target have the same violation, there is typically a problem at the target or its network infrastructure. Check the [Route Visualization](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-routes) to determine which network hops were common to all violating paths prior to and during the violation event.

## Latency

Latency is the time it takes for a packet to go from a source to a target. (Read more about [latency violations](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_latency).)

* **Notification Type:** *<type, such as email or webhook>* sent to *<destination>*.
* **Threshold:** Alerts when latency is greater than *<n>* milliseconds for *<n>* minutes.
* **Typical causes:** 
  + Network congestion
  + Routing error or routing change (for example, re-routing a latency-sensitive voice path over a VPN rather than directly over the internet could increase latency).
* **Check:** [Network path performance charts](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=path-performance&appid=appneta&language=&format=rendered) for changes in Latency and determine when they occurred. If needed, expand the timeline to include time leading up to alert.
  + Do any changes correlate with network changes made at the same time?
  + If you see both a latency and RTT jump this is indicative of a route change.
* **Review** the [Route Visualization](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-routes) to confirm that the path is over the correct network infrastructure.
* **Review** [diagnostic tests](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-diagnostics) run during the violation event.
  + Check the Latency column on the [Data Details tab](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/network-performance-monitoring-delivery/delivery-results/delivery-diagnostics.html#title-diagnostics_data-and-voice-details-tabs). Look for unexpected jumps in Latency along the path, potentially indicating a heavily used network device.
  + Note that the cause of the unexpected jump in latency can be at the first hop reporting the jump, the previous hop, or any infrastructure in between the two.
* **Check:** [Whether other paths to the same target exhibit the same symptoms](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_determine-the-scope-and-source-of-a-network-path-alert).
  + If only one or a small number of paths to the same target have the same violation, there is typically a network issue localized to the source location or region for those paths.
  + If many or all paths to the same target have the same violation, there is typically a problem at the target or its network infrastructure. Check the [Route Visualization](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-routes) to determine which network hops were common to all violating paths prior to and during the violation event.

## MOS (Mean Opinion Score)

The Mean Opinion Score (MOS) is an estimate of the sound quality of a call on a scale of 1 to 5, where 5 is perfect. It is a function of loss, latency, and jitter. It also varies with voice codec and call load. MOS is often used as a catch-all indicator of voice performance degradation in place of separate jitter, loss, and other thresholds.

* **Notification Type:** *<type, such as email or webhook>* sent to *<destination>*.
* **Threshold:** Alerts when MOS is less than *<n>* for *<n>* minutes.
* **Typical causes:** 
  + Traffic congestion along the network path
  + An overloaded network device
  + Bad physical media
  + Flapping routes
  + Flapping load balancing
  + Name resolution issues
  + Routing error or routing change to a path with one of the issues listed above
* **Check:** [Network path performance charts](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=path-performance&appid=appneta&language=&format=rendered) for the path to look for drops in MOS and determine when they occurred. If needed, expand the timeline to include time leading up to alert.
  + Do any changes correlate with network changes made at the same time?
  + If MOS drops, we recommend investigating voice metrics like [Voice Loss](https://docs.google.com/document/d/1HVIR6eqZKJN8JVaxILV26W5NeZrzurT10QGaE8H_y_RS7A/edit?_gfid=docs_editor_frame&csrfToken=c0f4735515904913c9703ad7b0d87bb91e9cdbee8363d8a6d89c76d9bbe3bba9&fileUrl=https%3A%2F%2Fapi.box.com%2Ffsip%2Ffiles%2F928907430086&isInboundFsipRequest=true&jsh=m%3B%2F_%2Fscs%2Fabc-static%2F_%2Fjs%2Fk%3Dgapi.lb.en.y0xCMa4KeeI.O%2Fd%3D1%2Frs%3DAHpOoo8-3MGCaatZB3kdS5TpZdd-gOSBHg%2Fm%3D__features__&organizationType=BUSINESS&parent=https%3A%2F%2Fbroadcom.ent.box.com&previewUrl=https%3A%2F%2Fbroadcom.ent.box.com%2Ffile%2F928907430086&rpctoken=18565003&tpat=1!0Q07y36eU2KlFBRNFPiqotD_SVRqX_sFQunzw2LrRlQa3VjykmsfGKeTdY8Hi95ym6EK5-n1AKU3LRnw3KfogtLEjc3CWblFl3wIfq4Q8OYx9uz5vJxRqGhkYfc2pbAx6ouYol8uNQSdPoKH2d20Zfr0-QlpIc4HceP5LMFWhJqGd7IDeb2h_bTj38M2IU0WLPs1Rfns35YRoZ-cxiUUem0PsNz2uPK9ZtpFA280io_jnh1wJ_-ZZMjzpcx1HtKpCNYianoW5nD9J7S1AyhcLQ4cAmpNZHKw31CHgVWKSKXzYTwUmSMkKW3i6-N3fMLwe5yO2PX-4z6KRXCVSqGPP3awlY2BZOWA4LB0onXnmdK7uLcQc4viX9nQmf-FKLs21ygAvbyNm33RWYYgmW2kCap9Fr6RHjcUTQRe04YZvJ3P7QvSC8RRipQ.&tpatExpirationTime=1707248496000&usegapi=1#heading=h.3jtnz0s) and [Voice Jitter](https://docs.google.com/document/d/1HVIR6eqZKJN8JVaxILV26W5NeZrzurT10QGaE8H_y_RS7A/edit?_gfid=docs_editor_frame&csrfToken=c0f4735515904913c9703ad7b0d87bb91e9cdbee8363d8a6d89c76d9bbe3bba9&fileUrl=https%3A%2F%2Fapi.box.com%2Ffsip%2Ffiles%2F928907430086&isInboundFsipRequest=true&jsh=m%3B%2F_%2Fscs%2Fabc-static%2F_%2Fjs%2Fk%3Dgapi.lb.en.y0xCMa4KeeI.O%2Fd%3D1%2Frs%3DAHpOoo8-3MGCaatZB3kdS5TpZdd-gOSBHg%2Fm%3D__features__&organizationType=BUSINESS&parent=https%3A%2F%2Fbroadcom.ent.box.com&previewUrl=https%3A%2F%2Fbroadcom.ent.box.com%2Ffile%2F928907430086&rpctoken=18565003&tpat=1!0Q07y36eU2KlFBRNFPiqotD_SVRqX_sFQunzw2LrRlQa3VjykmsfGKeTdY8Hi95ym6EK5-n1AKU3LRnw3KfogtLEjc3CWblFl3wIfq4Q8OYx9uz5vJxRqGhkYfc2pbAx6ouYol8uNQSdPoKH2d20Zfr0-QlpIc4HceP5LMFWhJqGd7IDeb2h_bTj38M2IU0WLPs1Rfns35YRoZ-cxiUUem0PsNz2uPK9ZtpFA280io_jnh1wJ_-ZZMjzpcx1HtKpCNYianoW5nD9J7S1AyhcLQ4cAmpNZHKw31CHgVWKSKXzYTwUmSMkKW3i6-N3fMLwe5yO2PX-4z6KRXCVSqGPP3awlY2BZOWA4LB0onXnmdK7uLcQc4viX9nQmf-FKLs21ygAvbyNm33RWYYgmW2kCap9Fr6RHjcUTQRe04YZvJ3P7QvSC8RRipQ.&tpatExpirationTime=1707248496000&usegapi=1#heading=h.184mhaj) first to determine what impacted the MOS change.
* **Review** the [Route Visualization](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-routes) to confirm that the path is over the correct network infrastructure.
* **Review** [diagnostic tests](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-diagnostics) run during the violation event.
  + Check the MOS column on the [Voice Details tab](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/network-performance-monitoring-delivery/delivery-results/delivery-diagnostics.html#title-diagnostics_data-and-voice-details-tabs). Look for significant drops in MOS along the path, potentially indicating a heavily used network device.
  + Note that the cause of the drop on MOS can be at the first hop reporting the drop, the previous hop, or any infrastructure in between the two.
* **Check:** [Whether other paths to the same target exhibit the same symptoms](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_determine-the-scope-and-source-of-a-network-path-alert).
  + If only one or a small number of paths to the same target have the same violation, there is typically a network issue localized to the source location or region for those paths.
  + If many or all paths to the same target have the same violation, there is typically a problem at the target or its network infrastructure. Check the [Route Visualization](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-routes) to determine which network hops were common to all violating paths prior to and during the violation event.

## QoS Change

Quality of Service ([QoS](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/network-performance-monitoring-delivery/delivery-results-overview/delivery-trupath.html#title-understanding-network-monitoring_qos)) markings on packets are used to prioritize traffic (for example, voice and video traffic). For priority traffic, if these markings are altered by a device in the network, a poor user experience can occur.

* **Notification Type:** *<type, such as email or webhook>* sent to *<destination>*.
* **Threshold:** Alerts when QoS markings are altered by the network. See [Alerting on QoS Changes](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=delivery-qos-alerts&appid=appneta&language=&format=rendered) for details.
* **Typical causes:** A network device that actively changes, removes, or doesn’t honor QoS markings.
* **Review** [diagnostic tests](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-diagnostics) run during the violation event.
  + Check the QoS column on the [Data Details tab](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/network-performance-monitoring-delivery/delivery-results/delivery-diagnostics.html#title-diagnostics_data-and-voice-details-tabs). Look for changes in QoS markings along the path.
  + Note that the cause of the QoS change can be at the first hop reporting the change, the previous hop, or any infrastructure in between the two.
* **Check:** [Whether other paths to the same target exhibit the same symptoms](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_determine-the-scope-and-source-of-a-network-path-alert).
  + If only one or a small number of paths to the same target have the same violation, there is typically a network issue localized to the source location or region for those paths.
  + If many or all paths to the same target have the same violation, there is typically a problem at the target or its network infrastructure. Check the [Route Visualization](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-routes) to determine which network hops were common to all violating paths prior to and during the violation event.

## Round Trip Time (RTT)

[Round Trip Time](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/network-performance-monitoring-delivery/delivery-results-overview/delivery-trupath.html#title-understanding-network-monitoring_round-trip-time-rtt-and-latency) (RTT) is the time it takes for a packet to go from a source to a target and back (the RTT chart in AppNeta shows the average RTT over the selected period). (Read more about [RTT violations](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_rtt).)

* **Notification Type:** *<type, such as email or webhook>* sent to *<destination>*.
* **Threshold:** Alerts when RTT is greater than *<n>* milliseconds for *<n>* minutes.
* **Typical causes:** 
  + Network congestion
  + Routing error or routing change (for example, re-routing a latency-sensitive voice path over a VPN rather than directly over the internet could increase latency)
* **Check:** [Network path performance charts](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=path-performance&appid=appneta&language=&format=rendered) for changes in RTT and determine when they occurred. If needed, expand the timeline to include time leading up to alert.
  + Do any changes correlate with network changes made at the same time?
  + If you see both a latency and RTT jump this is indicative of a route change.
* **Review** the [Route Visualization](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-routes) to confirm that the path is over the correct network infrastructure.
* **Review** [diagnostic tests](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-diagnostics) run during the violation event.
  + Check the RTT column on the [Data Details tab](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/network-performance-monitoring-delivery/delivery-results/delivery-diagnostics.html#title-diagnostics_data-and-voice-details-tabs). Look for unexpected jumps in RTT along the path, potentially indicating a heavily used network device.
  + Note that the cause of the unexpected jump in RTT can be at the first hop reporting the jump, the previous hop, or any infrastructure in between the two.
* **Check:** [Whether other paths to the same target exhibit the same symptoms](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_determine-the-scope-and-source-of-a-network-path-alert).
  + If only one or a small number of paths to the same target have the same violation, there is typically a network issue localized to the source location or region for those paths.
  + If many or all paths to the same target have the same violation, there is typically a problem at the target or its network infrastructure. Check the [Route Visualization](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-routes) to determine which network hops were common to all violating paths prior to and during the violation event.

## Voice Jitter

Jitter, also known as packet delay variation, is a measure of variation in latency. Jitter affects time-sensitive applications that use UDP but does not affect applications using TCP. Voice jitter is measured when packet trains emulating voice traffic (smaller payloads with wider packet spacing) are used for monitoring.

* **Notification Type:** *<type, such as email or webhook>* sent to *<destination>*.
* **Threshold:** Alerts when voice jitter is greater than *<n>* milliseconds for *<n>* minutes.
* **Typical causes:** 
  + Network congestion
  + Lack of QoS configuration
  + Mis-configured QoS
  + Network devices changing QoS markings
* **Check:** [Network path performance charts](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=path-performance&appid=appneta&language=&format=rendered) for changes in Jitter and determine when they occurred. If needed, expand the timeline to include time leading up to alert.
  + Do any changes correlate with network changes made at the same time?
* **Check:** If test packets are [configured to use the QoS markings](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=delivery-qos-templates&appid=appneta&language=&format=rendered) used by the traffic being emulated.
* **Review** [diagnostic tests](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-diagnostics) run during the violation event.
  + Check the QoS column on the [Data Details tab](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/network-performance-monitoring-delivery/delivery-results/delivery-diagnostics.html#title-diagnostics_data-and-voice-details-tabs). Make sure that the QoS markings are consistent (not being changed or dropped) along the path.
  + Check the Voice Jitter and Latency columns on the [Voice Details tab](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/network-performance-monitoring-delivery/delivery-results/delivery-diagnostics.html#title-diagnostics_data-and-voice-details-tabs). Look for significant jumps in Voice Jitter or Latency along the path indicating a source of congestion.
  + Note that the cause of the unexpected jump in jitter can be at the first hop reporting the jump, the previous hop, or any infrastructure in between the two.
* **Check:** [Whether other paths to the same target exhibit the same symptoms](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_determine-the-scope-and-source-of-a-network-path-alert).
  + If only one or a small number of paths to the same target have the same violation, there is typically a network issue localized to the source location or region for those paths.
  + If many or all paths to the same target have the same violation, there is typically a problem at the target or its network infrastructure. Check the [Route Visualization](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-routes) to determine which network hops were common to all violating paths prior to and during the violation event.

## Voice Loss

* **Notification Type:** *<type, such as email or webhook>* sent to *<destination>*.
* **Threshold:** Alerts when *<n>*% of voice packets are lost in tests occurring for *<n>* minutes.
* **Typical causes:** 
  + Traffic congestion along the network path
  + An overloaded network device
  + Bad physical media
  + Flapping routes
  + Flapping load balancing
  + Name resolution issues
  + Firewall protecting against DDOS resulting in a loss plateau (e.g., exactly 50% loss)
  + Selected target does not respond well to test packets
* **Check:** [Network path performance charts](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=path-performance&appid=appneta&language=&format=rendered) for changes in Voice Loss and determine when they occurred. If needed, expand the timeline to include time leading up to alert.
  + Do any changes in Voice Loss correlate with network changes made at the same time?
* **Review** [diagnostic tests](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-diagnostics) run during the violation event.
  + Check the Voice Loss column on the [Voice Details tab](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/network-performance-monitoring-delivery/delivery-results/delivery-diagnostics.html#title-diagnostics_data-and-voice-details-tabs). Look for a hop reporting non-zero voice loss that continues to be reported at all subsequent hops along the route.
  + Note that the cause of voice loss can be at the first hop reporting voice loss, the previous hop, or any infrastructure in between the two.
* **Check:** [Whether other paths to the same target exhibit the same symptoms](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_determine-the-scope-and-source-of-a-network-path-alert).
  + If only one or a small number of paths to the same target have the same violation, there is typically a network issue localized to the source location or region for those paths.
  + If many or all paths to the same target have the same violation, there is typically a problem at the target or its network infrastructure. Check the [Route Visualization](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-routes) to determine which network hops were common to all violating paths prior to and during the violation event.

# Web App Monitoring Alert Runbooks

These runbook templates cover how to handle an alert or notification triggered by Web Path violations.

## Apdex Score Violation

Apdex is an industry-standard method for reporting and comparing application performance in terms of end user experience. Apdex uses a simple formula to calculate user satisfaction. AppNeta presents the Apdex score as a percentage from 0% to 100%. Note that Apdex is averaged over a 2 hour window so the alert can take longer to clear than other alerts. See [Apdex documentation](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=experience-apdex&appid=appneta&language=&format=rendered) for further details.

* **Notification Type:** *<type, such as email or webhook>* sent to *<destination>*.
* **Threshold**: Alerts when the rolling average of Apdex scores falls below *<score>* for *<n>* tests.
* **Typical causes:** 
  + Application performance issues (for example, slow web app server).
  + Network performance problems (for example, network congestion or DNS issues).
* **Review** the [web path performance charts](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=web-path-charts&appid=appneta&language=&format=rendered) for the web path that generated the alert. If needed, [adjust the chart timeline](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/web-application-performance-monitoring-experience/experience-charts.html#title-web-path-details_adjust-chart-timeline) to include the time leading up to the alert.
* **Check:** The web path’s [DNS chart](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/web-application-performance-monitoring-experience/experience-charts.html#title-web-path-details_dns-chart) for issues with DNS server availability or slow response.
* **Check:** The End User Experience and Milestone Breakdown charts for end user experience time components (network, server, browser) or milestones taking more time than expected.
  + If the network time is longer than expected, check the [network path performance charts](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=path-performance&appid=appneta&language=&format=rendered) for network problems.
  + Otherwise, review individual [web path tests](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/web-application-performance-monitoring-experience/experience-charts.html#title-web-path-details_web-path-tests) during the issue to identify the resource(s) causing the component or milestone to take longer than expected.
* **Check** [whether other web paths to the same target exhibit the same symptoms](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/web-application-performance-monitoring-experience/experience-charts.html#title-web-path-details_comparing-web-path-performance).
  + If only one or a small number of paths to the same target have the same violation, there is typically an issue localized to the source location or region for those paths.
* **Check** whether the script on the violating path(s) has changed.
  + If many or all paths to the same target have the same violation, there is typically a problem at the target (web app) or its network infrastructure. Check the [Route Visualization](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-routes) to determine which network hops were common to all violating paths prior to and during the violation event.

## Connectivity Loss (Web Path)

Web path connectivity refers to the ability of a user on a browser (or script emulating a user) to access a web app. Web path connectivity alerts are generated when the script running on the Monitoring Point cannot connect to the target web app.

* **Notification Type:** *<type, such as email or webhook>* sent to *<destination>*.
* **Threshold:** Alerts triggered when the script cannot connect to the target web app over TCP for *<n>* tests.
* **Typical causes:** 
  + Network connectivity is lost.
  + There is a problem resolving the web app IP address using its hostname (DNS issue).
  + The web app is not running.
  + There is a web app infrastructure problem (for example, authentication services are down).
  + There is a routing problem.
* **Check** [whether other web paths to the same target exhibit the same symptoms](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/web-application-performance-monitoring-experience/experience-charts.html#title-web-path-details_comparing-web-path-performance).
* If only one or a small number of paths to the same target have lost connectivity to the web app, there is typically an issue localized to the source location or region for those paths.
  + Check whether the script on the violating path(s) has changed.
  + Check network path connectivity for the Delivery paths between the same source and target.
  + If network connectivity is lost, check the [Route Visualization](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-routes) for the network path(s), looking specifically at the TCP route, to see where and when the break in connectivity occurred. Also check the TCP route as that is the one the web app is taking.
* If many or all paths to the same target have lost connectivity to the same web app, there is typically a problem at the target (web app) or its network infrastructure.
  + Check the [Route Visualization](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-routes) to determine which network hops were common to all violating paths prior to and during the violation event.
* Try accessing the web app from your browser (to confirm that the target web app is available). Typical issues include:
  + There is a problem resolving the web app IP address using its hostname. This is a DNS issue (see the [DNS chart](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/web-application-performance-monitoring-experience/experience-charts.html#title-web-path-details_dns-chart)).
  + The web app is not running.
  + There is a web app infrastructure problem (for example, authentication services are down).

## HTTP Errors

HTTP errors are responses to HTTP requests that indicate a problem. An HTTP Error alert can be triggered if an HTTP Status of 4xx (client error) or 5xx (server error) is returned.

* **Notification Type:** *<type, such as email or webhook>* sent to *<destination>*.
* **Threshold:** Alerts triggered when the HTTP status returned by a script execution is 4xx (client errors) or 5xx (server errors) for *<n>* tests.
* **Typical causes:** 
  + Incorrect target URL used in the script or other script related problems.
  + Web app is down but its infrastructure is still up.
  + Changes to the web app are not reflected in the script.
* **Review** the script and the web app.
  + Has the monitoring script changed? Check the [historical web path status timeline](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/web-application-performance-monitoring-experience/experience-web-path-status.html#title-web-path-status_view-historical-web-path-status)) for a script change event (indicated by a purple diamond ♦) at the time of the HTTP Error alert. Review script changes and update as appropriate. For Selenium scripts, review the [Resolving Common Issues](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=experience-troubleshoot-selenium&appid=appneta&language=&format=rendered) page for hints on common scripting problems.
  + Has the web app changed? If so, review changes and update script as appropriate.
  + Is the web app available? Confirm that it can be accessed from a browser. If not, inform the team responsible for it.
  + Is it out of service due to scheduled maintenance? If so, wait for maintenance to complete.
* **Check:** [whether other web paths to the same target exhibit the same symptoms](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/web-application-performance-monitoring-experience/experience-charts.html#title-web-path-details_comparing-web-path-performance).
  + If only one or a small number of paths to the same target have the same violation, there is typically an issue localized to the source location or region for those paths.
    - Check whether the script on the violating path(s) has changed.
  + If many or all paths to the same target have the same violation, there is typically a problem at the target (web app) or its network infrastructure. Check the [Route Visualization](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-routes) to determine which network hops were common to all violating paths prior to and during the violation event.

## HTTP Status Violation

When a request is made to a target web app its response contains an HTTP Status. HTTP Status alerts occur when an unexpected HTTP Status is returned. Using this alert threshold is rare and tends to have specific applications. For example, expect a 403 status when accessing a protected resource and alert if it ever returns something different.

* **Notification Type:** *<type, such as email or webhook>* sent to *<destination>*.
* **Threshold:** Alerts triggered when an unexpected HTTP status is returned by the target for *<n>* tests.
* **Typical causes:** A change to the script or web app.
* **Check:** Review the script and the web app.
  + Is the expected HTTP status correct? If not, determine why the wrong HTTP status is being returned.
  + Has the script changed? If so, review script changes and update as appropriate. For Selenium scripts, review the [Resolving Common Issues](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=experience-troubleshoot-selenium&appid=appneta&language=&format=rendered) page for hints on common scripting problems.
  + Has the web app changed? If so, review changes and update script as appropriate.
  + Is the web app available? Confirm that it can be accessed from a browser. If not, inform the team responsible for it.
* **Check:** [Whether other web paths to the same target exhibit the same symptoms](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/web-application-performance-monitoring-experience/experience-charts.html#title-web-path-details_comparing-web-path-performance).
  + If only one or a small number of paths to the same target have the same violation, there is typically an issue localized to the source location or region for those paths.
    - Check whether the script on the violating path(s) has changed.
  + If many or all paths to the same target have the same violation, there is typically a problem at the target (web app) or its network infrastructure. Check the [Route Visualization](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-routes) to determine which network hops were common to all violating paths prior to and during the violation event.

## Page Load Time Violation

Page Load Time is the time it takes for a web page to render.

* **Notification Type:** *<type, such as email or webhook>* sent to *<destination>*.
* **Threshold:** alerts triggered when the time for a page to load is longer than *<n>* milliseconds for *<n>* tests.
* **Typical causes:** 
  + Web app issues or slowness on the web app server.
  + Script or web app change.
  + Network congestion.
  + Routing issues. Using the wrong (slower) route.
  + DNS issues. Slow DNS response.
* **Review** the [web path performance charts](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=web-path-charts&appid=appneta&language=&format=rendered) for the web path that generated the alert. If needed, [adjust the chart timeline](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/web-application-performance-monitoring-experience/experience-charts.html#title-web-path-details_adjust-chart-timeline) to include the time leading up to the alert.
* **Check** the [DNS chart](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/web-application-performance-monitoring-experience/experience-charts.html#title-web-path-details_dns-chart) for issues with DNS server availability or slow response.
* **Check** the End User Experience and Milestone Breakdown charts looking for end user experience time components (network, server, browser) or milestones taking more time than expected.
  + If the network time is longer than expected, check the [network path performance charts](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=path-performance&appid=appneta&language=&format=rendered) for network problems.
  + Otherwise, review individual [web path tests](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/web-application-performance-monitoring-experience/experience-charts.html#title-web-path-details_web-path-tests) during the issue to identify the resource(s) causing the component or milestone to take longer than expected.
* **Check:** [Whether other web paths to the same target exhibit the same symptoms](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/web-application-performance-monitoring-experience/experience-charts.html#title-web-path-details_comparing-web-path-performance).
  + If only one or a small number of paths to the same target have the same violation, there is typically an issue localized to the source location or region for those paths.
    - Check whether the script on the violating path(s) has changed.
  + If many or all paths to the same target have the same violation, there is typically a problem at the target or its network infrastructure. Check the [Route Visualization](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-routes) to determine which network hops were common to all violating paths prior to and during the violation event.

## Script Errors

A Script Error indicates a problem with a script or web app. For example, an element id specified in a script is not present on the page being accessed.

* **Notification Type:** *<type, such as email or webhook>* sent to *<destination>*.
* **Threshold:** Alerts when a problem with the script or the target web app is present for *<n>* tests.
* **Typical causes:** 
  + An element referenced in the script is not present on the page being accessed.
  + A command used in the script is not valid or is used improperly.
  + Invalid credentials are used in the script.
* **Check:** The [Web Drill-down page](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/web-application-performance-monitoring-experience/experience-charts.html#title-web-path-details_web-path-tests) at the time of the error. The error message and snapshot will provide clues to the cause of the problem.
  + For script issues, [test the Selenium script](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/set-up-monitoring/experience-deploy/experience-scripting/experience-scripting-selenium.html#title-selenium-scripting_test-the-script-in-apm) running on the web path and make changes as necessary.
  + For Selenium scripts, try using the [“captureEntirePageScreenshot” command](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/set-up-monitoring/experience-deploy/experience-scripting/experience-scripting-selenium-issues.html#title-resolving-common-issues_general-troubleshooting-technique) to help with debugging.

## Transaction Time Violation

Transaction time is the time it takes for a script test to complete.

* **Notification Type:** *<type, such as email or webhook>* sent to *<destination>*.
* **Threshold:** Alerts triggered when the time for the script to complete is longer than *<n>* milliseconds for *<n>* tests.
* **Typical causes:**
  + Web app issues. Slowness on the web app server or services that the app is dependent on (for example, an authentication provider, CDN provider, or in-site video links).
  + Script or web app change.
  + Network congestion.
  + Routing issues. Using the wrong (slower) route.
  + DNS issues. Slow DNS response.
* **Check:** [Compare multiple web paths that target the same app](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/web-application-performance-monitoring-experience/experience-charts.html#title-web-path-details_comparing-web-path-performance). Check for similar spikes in Transaction time across all web paths targeting that app. This indicates slowness on the web app server or services that the app is dependent on.
* **Check** for [Page Load Time alerts](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_page-load-time) on the same web path you received the Transaction Time alert. One or more slow page loads could cause the transaction time to be longer than expected.
* **Review** the script. If the script uses a waitFor command and the elements it is waiting for are either not present or are not loading, the transaction will take longer than expected.
* **Review** the [web path performance charts](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=web-path-charts&appid=appneta&language=&format=rendered) for the web path that generated the alert. If needed, [adjust the chart timeline](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/web-application-performance-monitoring-experience/experience-charts.html#title-web-path-details_adjust-chart-timeline) to include the time leading up to the alert.
* **Check** the [DNS chart](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/web-application-performance-monitoring-experience/experience-charts.html#title-web-path-details_dns-chart) for issues with DNS server availability or slow response.
* **Check** the End User Experience and Milestone Breakdown charts looking for end user experience time components (network, server, browser) or milestones taking more time than expected.
  + If the network time is longer than expected, check the [network path performance charts](https://techdocs.broadcom.com/bin/gethidpage?ux-context-string=path-performance&appid=appneta&language=&format=rendered) for network problems.
  + Otherwise, review individual [web path tests](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/web-application-performance-monitoring-experience/experience-charts.html#title-web-path-details_web-path-tests) during the issue to identify the resource(s) causing the component or milestone to take longer than expected.
* **Check:** [Whether other web paths to the same target exhibit the same symptoms](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/web-application-performance-monitoring-experience/experience-charts.html#title-web-path-details_comparing-web-path-performance).
  + If only one or a small number of paths to the same target have the same violation, there is typically an issue localized to the source location or region for those paths.
    - Check whether the script on the violating path(s) has changed.
  + If many or all paths to the same target have the same violation, there is typically a problem at the target or its network infrastructure. Check the [Route Visualization](https://techdocs.broadcom.com/us/en/ca-enterprise-software/it-operations-management/appneta/GA/analyze-results/investigating-violation-events.html#title-investigating-violation-events_use-routes) to determine which network hops were common to all violating paths prior to and during the violation event.

# Template Revision History

This section is designed to provide an overview of material changes to the AppNeta Customizable Runbook Templates document. As a general guideline, small semantic changes will not be tracked.

| **Version** | **Revision Month** | **Changes** |
| --- | --- | --- |
| 2.1 | March 2024 | * Added Technical Support section with placeholder for Site ID * Added section for User Provisioning in AppNeta * Added step to Monitoring Point runbooks to assign custom tags |
| 2.0 | February 2024 | * Simplified styling formats in document template. * Updated runbooks to configure network monitoring using monitoring policies instead of path template groups * Added an overview section for integrations, with a template for DX NetOps * Added terminology definitions for single-ended monitoring, dual-ended monitoring, network path |
| 1.5 | October 2023 | * Updated documentation links, copyright year. * Removed cpe5. Added cpe40 for Arista and CMP for GCP. * Removed step to assign licenses to Monitoring Points because they are now assigned automatically. * Removed step to rename a Monitoring Point because it is optional. * Removed step to set Monitoring Point locations because it is now automatically detected by default. |
| 1.4 | March 2022 | * Rebuilt document using Broadcom corporate template. * Updated product terminology from AppNeta Performance Manager (APM) to AppNeta. * Renamed and reorganized the Overview section. Reordered terminology. * Updated contact email to provide feedback on the document. |
| 1.3 | February 2022 | * Changed Support contact info. |
| 1.2 | December 2021 | * Added Change Log |
| 1.1 | November 2021 | * Revised hyperlinks. |
| 1.0 | November 2021 | * Initial document version. |

