Bitdefender®

Network Traffic Security Analytics

Installation and Administration Guide

LEGAL NOTICE

Warning and Disclaimer. This product and its documentation are protected by copyright. The information in this document is provided on an "as is" basis, without warranty. Although every precaution has been taken in the preparation of this document, the authors will not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

This book contains links to third-party websites that are not under the control of Bitdefender, therefore Bitdefender is not responsible for the content of any linked site. If you access a third-party website listed in this document, you will do so at your own risk. Bitdefender provides these links only as a convenience, and the inclusion of the link does not imply that Bitdefender endorses or accepts any responsibility for the content of the third-party site.

Trademarks. Trademark names may appear in this book. All registered and unregistered trademarks in this document are the sole property of their respective owners, and are respectfully acknowledged.

Bitdefender

Table of Content

1. Overview

1.1. Scope of This Document

This document is intended to guide the system / network / security administrators throughout the Bitdefender Network Traffic Security Analytics (NTSA) solution setup and configuration process.

You will also find hereinafter a comprehensive description of the Bitdefender NTSA solution and all the information you need to know for installing and using it to monitor your network activity.

1.2. About Bitdefender Network Traffic Security Analytics

1.2.1. What It Is

Bitdefender Network Traffic Security Analytics (NTSA) is a network security solution that analyzes IPFIX traffic streams for the presence of malicious behavior and malware.

Bitdefender NTSA is meant to act alongside your existing security measures as a complementary safeguard that is capable of covering the blind spots that traditional tools do not monitor.

Traditional network security tools generally attempt to prevent malware infections by inspecting inbound traffic (via sandbox, firewalls, antivirus and so on). Bitdefender NTSA focuses solely on monitoring outbound network traffic for malicious behavior.

The solution consists of two components: **Bitdefender Network Traffic Security Analyzer** and **Bitdefender Probe**. Bitdefender provides these components as virtual appliances, which you can deploy in your virtual environment.

- **Bitdefender Network Traffic Security Analyzer**: hosts an internal web interface, allowing you to configure settings and monitor the alerts.
- **Bitdefender Probe**: has access to the full-packet stream, requires no dedicated internet connectivity and has no onboard data storage.

1.2.2. How Does It Work

To detect malware, Bitdefender NTSA monitors all connections to the internet using a Bitdefender Probe installed in your network. The Bitdefender Probe is responsible for extracting metadata (flow data) from network traffic and sending it in IPFIX format to the Bitdefender Network Traffic Security Analyzer, which detects malware by analyzing these data.

Bitdefender NTSA never looks at your confidential data; it only analyzes your traffic metadata characteristics without requiring data decryption, thus maintaining the data privacy.

Bitdefender NTSA continuously analyzes metadata using the **Intelligence Driven Egress Security Model** against a list of internet addresses known to communicate with malware.

For detecting malicious behavior over a longer time, the Bitdefender Network Traffic Security Analyzer uses heuristic analysis of traffic data, including the destinations, behaviors and patterns in network traffic. This feature provides the Bitdefender Network Traffic Security Analyzer with a more fine-grained detection method, designed to capture malware that slips through security product implementations limited to real-time detection. The heuristic analysis of network traffic is part of Bitdefender **Cyber Threat Intelligence (CTI),** a large database of malicious indicators built and updated using a combination of partner feeds, commercial feeds and open sources. Approximately 100.000 updates are processed every hour.

Bitdefender NTSA operates parallel to the network infrastructure and has no impact on network performance. The Bitdefender Probe filters all content using mirrored traffic (SPAN data), keeping only the metadata. The Bitdefender Probe sends these data to the Bitdefender Network Traffic Security Analyzer, where all metadata is stored (forensically) and analyzed (using CTI).

The Bitdefender Network Traffic Security Analyzer raises an alert and informs the user which devices are probably infected and which ones are certainly infected. It verifies the probably infected devices and alerts about any suspected malware activity to keep an eye on.

2. Installation and Setup

The Bitdefender NTSA solution consists of two components, available as virtual appliances in OVA format:

- **Bitdefender Network Traffic Security Analyzer**, which analyzes the exported flow data and reports any detection.
- **Bitdefender Probe**, which extracts metadata from network traffic (mirrored / SPAN data) and transports them to the Bitdefender Network Traffic Security Analyzer.

You can install and use the Bitdefender NTSA solution on the company's premises, without any impact on the network infrastructure performance. Bitdefender NTSA simply feeds on flow-data from your router. This data processing does not require external resources and does not affect the internal network traffic or internet-related activities.

The appliances are effective immediately after installation. Bitdefender NTSA loads the latest malicious indicators when powered on. Relevant alerts are generated instantly, pinpointing compromised devices in your network.

Before starting to install the solution, make sure your environment complies with Bitdefender NTSA installation requirements.

The solution installation and setup process includes the following steps:

1. Create a host-internal virtual network
2. Install and configure Bitdefender Network Traffic Security Analyzer
3. Install and configure the Bitdefender Probe

2.1. Installation Requirements

2.1.1. Virtual Appliances Requirements

Bitdefender Network Traffic Security Analyzer Requirements

- Virtualization platform: VMware ESXi 5.0 & higher
- Storage capacity: 550 GB minimum / 550 GB recommended
- CPU cores: 8 minimum / 8 recommended
- RAM memory: 8 GB minimum / 8 GB recommended

Bitdefender Probe Minimum Requirements

- Virtualization platform: VMware ESXi 5.0 & higher
- Storage capacity: 8 GB
- CPU cores: 2
- RAM: 2 GB

2.1.2. Communication Requirements

- Bitdefender Network Traffic Security Analyzer needs Internet access via HTTP and HTTPS, for downloading the Cyber Threat Intelligence lists and the software updates.
- Bitdefender requires access from the NTSA appliance (eth0) to the download.bitdefender.com (port 443).
- For the NTSA remote support service to work, Bitdefender NTSA requires access to vpn-ntsa.bitdefender.com (port 443).
- Optionally, you may need DNS (UDP port 53), NTP (UDP port 123) and SMTP (TCP port 25) internet access, depending on the web interface settings.

2.1.3. Firewall Exceptions

Allow these destinations on your local firewall for the NTSA appliance:

- Bitdefender NTSA updates: download.bitdefender.com (port 443)
- Bitdefender NTSA support: vpn-ntsa.bitdefender.com (port 443)

Note

You can open a tunnel to allow Bitdefender Support to connect to your NTSA appliance. You can shut down this tunnel whenever you want, but it will automatically be shut down 24 hours after triggering it.
To enable Bitdefender Support to connect to your NTSA appliance, go to **Settings > Admin & System > Maintenance > Enable remote support (by VPN)**.

2.2. Creating a Host-Internal Network

For Bitdefender Network Traffic Security Analyzer to receive IPFIX traffic from the Bitdefender Probe, they both must be connected to the same host-internal virtual network. It is recommended to create this host-internal network first, for the installation to go smoothly.

To create a host-internal network for connectivity between Bitdefender Probe and NTSA appliances:

1. In your virtualization client (VMware vSphere Client), select the host from the left-side panel.
2. Go to the **Configuration** tab and select **Networking > Add networking…**
3. Keep the default connection type (**Virtual Machine**) and click **Next**.
4. Select **Create a vSphere standard switch** and uncheck all virtual Network Interface Cards (NICs) to create the network host-internal. Click **Next**.
5. Provide the newly added network with a specific name (for example, `bitdefender-ntsa`).
6. Click **Next** and complete the wizard.

2.3. Installing and Setting Up the Bitdefender Network Traffic Security Analyzer

2.3.1. Deploying the Bitdefender Network Traffic Security Analyzer Appliance

Bitdefender Network Traffic Security Analyzer is delivered in the Open Virtualization Format (OVF) and Virtual Hard Disk Drive (VHD), allowing for easy deployment in any modern virtualization hypervisor.

Follow the deployment steps based on your virtualization solution.

VMware vSphere

Microsoft Hyper-V

VMware vSphere

To deploy the appliance, download the NTSA OVA file and perform the following steps in VMware vSphere Client for Windows:

1. Open VMware vSphere Client and select **File > Deploy OVF Template**.
2. Select the OVA file you have downloaded from the Bitdefender NTSA website.
3. Click **Next** to go through the wizard and make the required configurations. We recommend using thick disk formats (default setting).

Microsoft Hyper-V

To deploy the appliance, download the NTSA VHD file and perform the following steps in Microsoft Hyper-V:

1. Place the file in the destination path for Hyper-V images.

   By default, the location is: C:\Users\Public\Documents\Hyper-V\Virtual hard disks
2. Open Hyper-V Manager GUI.
3. In the **Actions** sidebar, click **New**.
4. Enter a name for the VM such as *NTSA*.
5. (Optional) Choose a non-default location to store VM configuration files.
6. Choose **Generation 1** as a **VM type**.

   NTSA is built as a non-EFI compatible legacy bios boot image.
7. Assign **8192 MB** as **Startup Memory**. The NTSA runs with less during the setup phase. It is recommended to start with this RAM amount and turn **on Dynamic Memory** to downscale, if idle.
8. Select the **Management Network Adapter**.
9. Select **Use an existing virtual hard disk** and choose the downloaded NTSA VHD file.
10. Review the summary and click **Finish**.
11. Go to **Virtual Switch Manager**.

12. Create a dedicated IPFIX network (Internal Network).

    Skip this step if the Probe is located outside the Hyper-V cluster.
13. In the **Actions** sidebar, select the newly created VM.
14. Select **Settings**.
15. Configure three more network adapters, connected to the IPFIX network.

    Create the adapters as placeholders, without uplinking. These may be needed in the future.
16. Go to **Memory** and modify the **Dynamic Memory** ranges to **2048 minimum** and **8192 Maximum**.
17. Close **Settings** and boot the NTSA VM.

2.3.2. Setting Up the Bitdefender Network Traffic Security Analyzer

Power on Bitdefender Network Traffic Security Analyzer in VMware vSphere Client and access its settings. You will notice that the Bitdefender Network Traffic Security Analyzer has four network adapters:

- **Network adapter 1 / Port 0 / eth0**: initial configuration interface.
- **Network adapter 2 / Port 1 / eth1**: management interface.
- **Network adapter 3 / Port 2 / eth2**: flow data interface.
- **Network adapter 4 / Port 3 / eth3**: special-purpose interface. Not used by default.

Access the **Console** tab of the Bitdefender Network Traffic Security Analyzer. The console displays the IP address for the NTSA web interface (network adapter 2) that was detected on boot-up, but only if it received a valid DHCP lease or if the IP configuration has been set statically.

Note

Changes will be taken into account on the console only after a reboot.

We will explain hereinafter how to connect all required network adapters to the virtual switches and interfaces on the hypervisor.

The Initial Configuration Interface (Network Adapter 1 / eth0)

The first network interface (eth0) is used for the initial network configuration of Bitdefender Network Traffic Security Analyzer. Connecting this interface to the hypervisor is only necessary when deploying a new appliance. To be able to reach the interface, which is configured with a static IP address (10.100.100.101 / 255.255.255.0), the interface needs to be connected to the same virtual switch as the VMware vSphere Client (named VM Network, by default).

To connect the interface eth0:

1. In the VMware vSphere Client, select the Bitdefender Network Traffic Security Analyzer appliance and open its settings.
2. On the **Hardware** tab, select **Network adapter 1 > Network Connection > VM Network**.
3. Click **OK** to confirm.

The Management Interface (Network Adapter 2 / eth1)

The management interface (eth1) of the Bitdefender Network Traffic Security Analyzer is used to connect to the Web interface of the appliance. To connect the management interface to an existing virtual switch:

1. In the VMware vSphere Client, select the Bitdefender Network Traffic Security Analyzer appliance and open its settings.
2. On the **Hardware** tab, select **Network adapter 2 > Network Connection > VM Network**.
3. Click **OK** to confirm.

In the case when Bitdefender Network Traffic Security Analyzer does not receive an IP address on eth1 (network adaptor 2), the NTSA processes are not started and the following line is displayed in red. Click `r` to refresh the screen.

```
rs-app: no, rs-web: no, collector: no, check PS
```

If all processes are started correctly, this specific line is colored in white:

```
rs-app: ok, rs-web: ok, collector: ok
```

In case DHCP is not available, you can assign an IP address to eth1 only once by pressing `n`.

The Flow Data Interface (Network Adapter 3 / eth2)

The role of the flow data interface (eth2) on Bitdefender Network Traffic Security Analyzer is to receive IPFIX traffic generated by flow exporters, such as the Bitdefender Probe.

For Bitdefender Network Traffic Security Analyzer to receive IPFIX traffic from the Bitdefender Probe, they both must be connected to the same host-internal virtual network. Configure Bitdefender Network Traffic Security Analyzer to communicate with the host-internal network as follows:

1. In VMware vSphere Client, select the Bitdefender Network Traffic Security Analyzer appliance and open its settings.
2. On the **Hardware** tab, select **Network adapter 3 > Network Connection**.
3. Select the host-internal network previously created.
4. Click **OK** to confirm.

2.4. Installing and Setting Up the Bitdefender Probe

2.4.1. Deploying the Bitdefender Probe Appliance

The Bitdefender Probe is a flexible device that can be installed in any network environment.

Follow the deployment steps based on your virtualization solution.

VMware vSphere

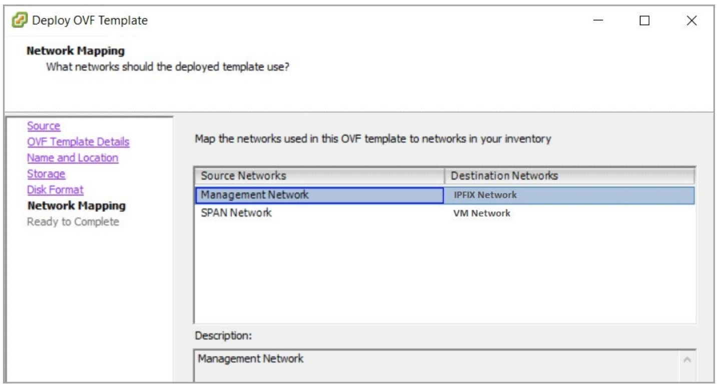
Microsoft Hyper-V

VMware vSphere

To deploy the appliance, download the Probe OVA file and perform the following steps in the VMware vSphere Client for Windows:

1. Open VMware vSphere Client and select **File > Deploy OVF Template**.
2. Select the Bitdefender Probe OVA file you have downloaded from the Bitdefender NTSA website.
3. Click **Next** to go through the wizard and make the required configurations. We recommend using thick disk formats (default setting).

   The Bitdefender Probe exhibits two types of network interfaces: monitoring or management. In the **Network Mapping** section, you can choose the destination networks from your inventory for the monitoring or management networks predefined in Bitdefender Probe template:



Network Mapping

What networks should the deployed template use?

Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
Management Network	IPFIX Network
SPAN Network	VM Network

Description:

Management Network

- **Management Network** is responsible for the Bitdefender Probe updates and communication with the NTSA appliance. It must be connected to the same network as the eth0 of NTSA appliance.
- **SPAN Network** is responsible for receiving SPAN data / mirrored network traffic. It must be connected to the network to be monitored.

Important

By default, the Probe downloads updates through the NTSA appliance. For the updates to work, the Probe must connect to the NTSA over the 10.200.200.0/24 range. For custom setups, it is mandatory to connect the Probe’s Management Network to a network with firewall rules that allow connections to download.bitdefender.com. In this case, the IPFIX data must be sent to the NTSA's management interface instead of the predefined 10.200.200.201.

he Bitdefender Probe is a flexible device that can be installed in any network enviro

Microsoft Hyper-V

To deploy the appliance, download the Probe VHD file and perform the following steps in Microsoft Hyper-V:

1. Log in to Hyper-V Manager.
2. Create a virtual switch (vSwitch) for the BD Probe traffic capture interface an name it **NTSA**.
3. Go to **Extensions** and enable **Microsoft NDIS Capture**.
4. Open PowerShell and configure mirroring mode on the external port of the vSwitch by running the following commands:

```
$Var=Get-VMSystemSwitchExtensionPortFeature –FeatureName
Ethernet Switch Port Security Settings"

$Var.SettingData.MonitorMode=2

Add-VMSwitchExtensionPortFeature -ExternalPort -SwitchName NTSA -
VMSwitchExtensionFeature $Var
```

Note

NTSA is the vSwitch, whereas **MonitorMode=2** is the source monitoring mode.

5. Create a Virtual Machine (VM) and configure the following settings:
   a. Select **Generation 1** for the VM.
   b. Assign **2048 MB** of memory.
   c. Connect the existing virtual hard disk BDProbe.vhd file to the virtual machine.
6. Click **Finish**.
7. Open the VM settings and add a new network adapter.
8. Connect the new network adapter to the NTSA vSwitch in step 2 and configure the following settings:
   a. Under **Port mirroring**, set **Mirroring mode** to **Destination**.
9. Click **Apply**.

2.4.2. Setting Up the Bitdefender Probe

You will learn hereinafter the following:

Configure the Bitdefender Probe settings

Connect the Bitdefender Probe management interfaces

Monitor internal data sources using Bitdefender Probe

Monitor external data sources using Bitdefender Probe

License the Bitdefender Probe

Configuring the Bitdefender Probe Settings

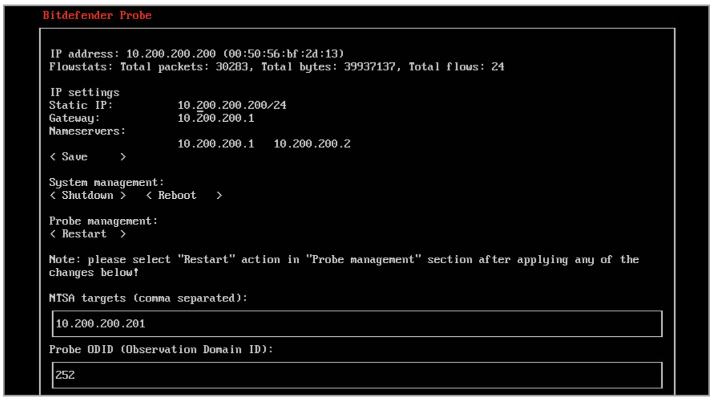
Power on the Bitdefender Probe appliance in VMware vSphere Client and access its settings.

You will notice that the Bitdefender Probe appliance has two virtual network adapters:

- **Network adapter 1 / eth0**: the Management Network virtual adapter. Default IP: 10.200.200.200.
- **Network adapter 2 / eth1**: SPAN Network virtual adapter.

Access the Bitdefender Probe TTY console in VMware vSphere Client, to configure the IP settings, NTSA targets and ODID.

- Click in the TTY screen to edit.
- Use the arrow keys to move between settings.
- After editing a setting, make sure to press the **Enter** key to apply.



```
Bitdefender Probe

IP address: 10.200.200.200 (00:50:56:bf:2d:13)
Flowstats: Total packets: 30283, Total bytes: 39937137, Total flows: 24

IP settings
Static IP:          10.200.200.200/24
Gateway:            10.200.200.1
Nameservers:
                    10.200.200.1   10.200.200.2
< Save     >

System management:
< Shutdown >   < Reboot    >

Probe management:
< Restart  >

Note: please select "Restart" action in "Probe management" section after applying any of the
changes below!

NTSA targets (comma separated):

 10.200.200.201

Probe ODID (Observation Domain ID):

 252
```

- The **Static IP**, **Gateway** and **Nameservers** must be within the defined Management Network.
- You can enter several NTSA targets (NTSA appliance IPs) separated by comma (without any spaces).
- The ODID (Observation Domain ID) may be defined between 0-252.
- After making changes, select the **<Restart>** option under **Probe management**.

Connecting the Bitdefender Probe Management Interfaces

The Bitdefender Probe management interfaces serve for NTP synchronization and flow data export. Therefore, you need to connect the Bitdefender Probe to the same host-internal virtual network as the Bitdefender Network Traffic Security Analyzer. Proceed as follows:

1. In VMware vSphere Client, select the deployed Bitdefender Probe appliance and open its settings.
2. On the **Hardware** tab, select **Network adapter 2**.

3. Go to the **Network Connection** on the right panel and select the host-internal network previously created.
4. Click **OK** to confirm.

The second network adapter of Bitdefender Probe is set by default to `10.200.200.200 / 255.255.255.0`. To establish a communication channel between the Bitdefender Probe and Bitdefender Network Traffic Security Analyzer, connect the flow data interface to the host-internal network and configure the respective flow data interface on the same subnet, for example, `10.200.200.201 / 255.255.255.0` (the Bitdefender Network Traffic Security Analyzer uses this IP configuration by default on the flow data interface).

Monitoring Internal Data Sources Using the Bitdefender Probe

To monitor internal data sources using the Bitdefender Probe, such as a virtual switch, proceed with the steps described hereinafter in the VMware vSphere Client.

Note
This procedure considers a setup in which all traffic flowing through the virtual switch is mirrored (for example, the switch is set to VLAN ID 4095, which includes all VLANs).

1. In the VMware vSphere Client, select the host from the left-side panel.
2. Go to the **Configuration** tab and select **Networking**.
3. Find the virtual switch you want to monitor and open its **Properties…**
4. Click **Add…** to create a new port group.
5. Keep **Virtual Machines** as the connection type and click **Next**.
6. Enter a name for the new port group (for example, based on which traffic is monitored).
7. For **VLAN ID**, select **All (4095)**.
8. Click **Next** to review the settings and **Finish** to confirm.

In the next phase, you will add one of the Bitdefender Probe monitoring network interfaces to the newly created port group:

1. In the VMware vSphere Client, select the Bitdefender Probe appliance and open its settings.
2. On the **Hardware** tab, select the monitoring network adapter**.**
3. In the right panel, under **Network Connection**, select the new port group.
4. Click **OK** to confirm.

Note
Since the Bitdefender Probe supports only 1 GbE (Gigabit Ethernet) network interfaces, the total amount of mirrored traffic should not exceed 1 GbE, otherwise, data loss may occur.

Monitoring External Data Sources Using the Bitdefender Probe

Besides monitoring virtual switches, the Bitdefender Probe may receive mirrored traffic from physical devices, such as switches and network Test Access Ports (TAPs). This configuration requires a virtual switch to which both the Bitdefender Probe and one (or more) physical network interfaces are connected. To configure the monitoring of external data sources using Bitdefender Probe:

1. In the VMware vSphere Client, select the host from the left-side panel.
2. Go to the **Configuration** tab and select **Add Networking…**
3. Keep **Virtual Machines** as the connection type and click **Next**.
4. Select **Create a vSphere standard switch** (default) and select one or more virtual machine Network Interface Cards (vmNICs) on which the mirrored traffic is to be received. Click **Next**.
5. Provide the newly added network with a specific name (for example, based on which traffic is monitored).
6. For **VLAN ID**, select **All (4095)**.
7. Click **Next** and complete the wizard.

The newly added switch must be set to **promiscuous mode**, to ensure that it accepts all mirrored traffic. Proceed as follows:

1. Select the new switch and open its **Properties.**
2. Select **vSwitch** on the **Ports** tab and click **Edit.**
3. In the virtual switch properties window, navigate to the **Security** tab.
4. Set **Promiscuous mode** to **Accept**.
5. Confirm the change by selecting **OK**.
6. **Close** the properties window.

The next step consists of adding one of the Bitdefender Probe monitoring network interfaces to the newly created port group:

1. In the VMware vSphere Client, select the deployed Bitdefender Probe appliance and open its settings.
2. On the Hardware tab, select the monitoring network adapter.
3. Go to the **Network Connection** on the right panel and select the new port group.
4. Click **OK** to confirm.

Note

Since the Bitdefender Probe supports only 1 GbE (Gigabit Ethernet) network interfaces, the total amount of mirrored traffic should not exceed 1 GbE, otherwise, data loss may occur.

Licensing the Bitdefender Probe

An unlicensed probe can send maximum 25000 data flows to the Bitdefender Network Traffic Security Analyzer appliances. After licensing the Bitdefender Probe, the number of sent flows will be unlimited.

You can license the Bitdefender Probe by entering the license keys in the license files available on the appliance.

Prerequisites:

- The Bitdefender Probe license keys provided by the Bitdefender team, corresponding to the base license, the DNS license and the HTTP license.
- An SSH client.

To license the Bitdefender Probe:

1. Connect to the defined Management Network IP using an SSH client.
2. Enter the default user: `bdadmin` and password: `awake`.
3. You will be prompted to change the default password, then re-enter the new password.
4. Open again the SSH client and connect to the same Management Network IP using the new password.
5. Use the following commands to enter the license keys in the appropriate license file (replace LICENSE_KEY with the respective license string):
   a. `echo "<LICENSE_KEY>" | sudo tee /etc/nprobe.license`
6. Access the Bitdefender Probe TTY console in VMware vSphere Client and select **<Restart>** under **Probe Management**, to apply the license changes.

Note
You can also apply the license using the following command in the SSH session: `sudo systemctl restart bdprobe.service`.

2.5. Configure the NTSA Components Communication

2.5.1. Configuring the Initial Access to the Web Interface

The Bitdefender Network Traffic Security Analyzer hosts an internal web interface to configure settings for the system. Initial access is supplied to 10.100.100.100 on network adapter 1 (**eth0**). To access the web interface, simply configure a system in this range (for example, make your client 10.100.100.101). Use any web browser to gain access, using `https://10.100.100.100` to connect to the web interface of the system.

For gaining initial access to the web interface:

1. Connect a client computer to **eth0**.
2. Configure a client system within the range of the system (for example, use 10.100.100.101, subnet mask 255.255.255.0 and no gateway) to access the login screen.
3. Connect to the management console with username `admin` and password `bitdefender default`. View the chapter Logging in to Web Console for more details.
4. In the management console, go to **Settings > Network > Internet and Flow Data** and assign the appropriate internet settings.

   Note
   To edit settings on any page of the console, click the icon ✎ next to the setting category name.
5. In the management console, go to **Settings > Maintenance > Reboot appliance** to restart the Bitdefender Network Traffic Security Analyzer. This operation will take several minutes.

6. Disconnect the client computer from **eth0** and connect Bitdefender Network Traffic Security Analyzer to your network using its management interface (**eth1**). The management interface will use the settings configured in step 4.

7. Access again the web interface using the internet address configured in step 4. Subsequently, use the default credentials to obtain access to the settings pages and continue with the configuration settings for networking, Syslog, HTTP proxy, IPFIX, SMTP alerts and detection.

   Note

   The fixed address on network adapter 1 is intended primarily to regain access to the unit if network adapter 2 is misconfigured. Network adapter 1, however, may still be used for further configuration after reboot.

2.5.2. Configuring Netflow

Next, you need to configure the flow data interface as follows:

1. Connect the Bitdefender Probe to the Bitdefender Network Traffic Security Analyzer on network adapter 3 (**eth2**). If there is only one probe in the configuration, the default setup is sufficient. If you use more probes, you need to configure the IPFIX interface on the Bitdefender Network Traffic Security Analyzer with the correct network setup.

2. Set the IP information of the **eth2** adapter in the web interface at **Settings > Network > Flow Data.** Because the flow data is sent over UDP, the interface on the Bitdefender Network Traffic Security Analyzer will only listen to incoming data. There is no need to configure a gateway, not even for configurations with multiple probes on different subnets and networks.

   Note

   Define an IP address in a different subnet than the IP address of **eth1** (the management interface).

3. In the management console, go to **Settings > Maintenance > Reboot appliance** to restart the Bitdefender Network Traffic Security Analyzer. This operation will take several minutes.

4. Configure the edge-router to supply the Bitdefender Network Traffic Security Analyzer with the Netflow stream:

   b. Login to the router and enter the following commands:

   ```
   enable
   configure terminal
   ```

   c. Assign the correct Netflow source IP address of the interface to the Netflow packets. This IP should be within the range of the Bitdefender Network Traffic Security Analyzer, to avoid packet drop:

   ```
   ip flow-export source <interface>
   ```

   d. Assign the Bitdefender Network Traffic Security Analyzer address as a Netflow destination using:

   `ip flow export destination <address> <port>` (use port 2055)

   If a Netflow export destination already exists, add this as an additional destination.

   e. Enable Netflow version 9 using:

```
ip netflow version 9
```

f. Use `ip inflow ingress` on the router's interface that receives internet traffic.

g. End the configuration process with the `end` command.

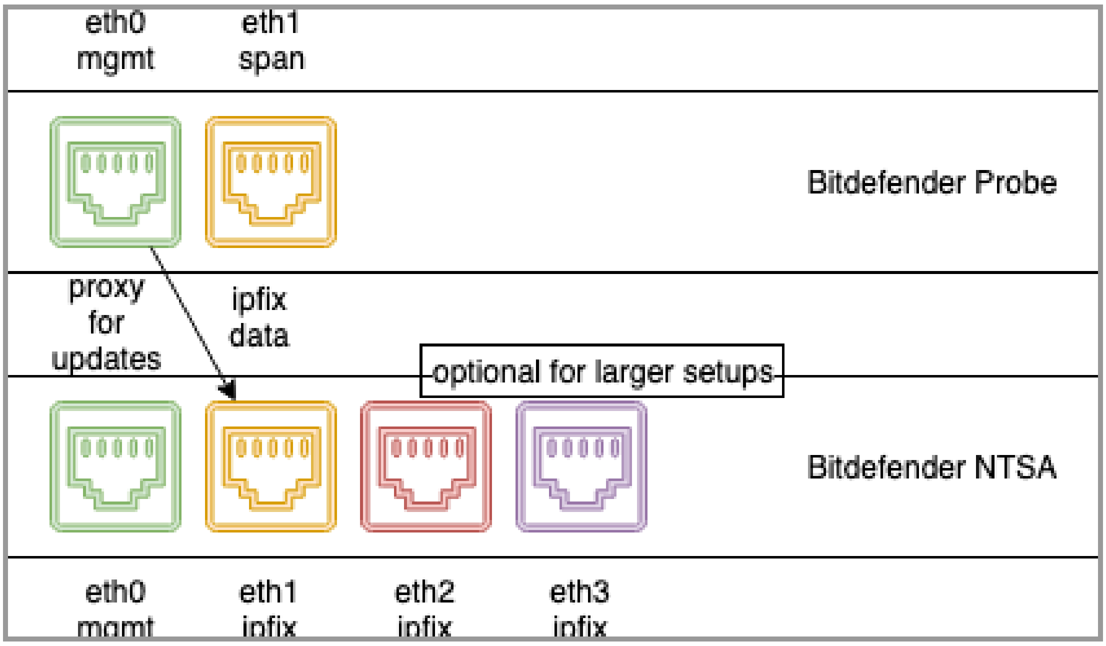
h. Check the configured settings with `show running-config` command.

i. Test connectivity and then save the changes to the router using the `write` command.

Note

For more information about Netflow configuration, refer to this CISCO web article.

A schematic overview of the Bitdefender Network Traffic Security Analyzer and the Bitdefender Probe is in the picture below:



Bitdefender NTSA

- eth0 : Management interface
- eth1 - IPFix interface - preconfigured static IP - 10.200.200.201
- eth2 - IPFix interface - preconfigured static IP - 10.200.202.202

eth3 - IPFix interface - preconfigured static IP - 10.200.203.203

Bitdefender Probe

- eth0 - IPFix interface - preconfigured static IP - 10.200.200.200
- eth1 - SPAN Data – listen network (interface)

eth 2 and eth 3 are not configurable through the Web Console.

Important

- The Bitdefender Network Traffic Security Analyzer needs internet access to load and update its internal threat intelligence lists and rules. For this, it needs access to the Bitdefender update servers on the Internet using port 443.
- The Bitdefender Network Traffic Security Analyzer needs to be able to query external DNS names. This is a necessary condition for the Bitdefender Network Traffic Security Analyzer engines.
- Optionally, NTP (UDP port 123) and SMTP (TCP port 25) internet access are needed, depending on the web interface settings.
- Additionally, if appropriate for configuring this system in your network, the HTTP proxy settings are used as defined in the web interface. The system uses the gateway supplied on network adapter 2 for internet access.

3. Monitoring your network

Monitoring and analysing the outgoing traffic before any NAT, filtering, firewalling, etc. enables Bitdefender Network Traffic Security Analyzer to:

- Perform the best possible **security analytics**, as the Bitdefender Network Traffic Security Analyzer receives complete metadata (IPFIX data).
- **Resolve hostnames** related to IP addresses based on DNS (if available) enabling the system administrators to locate and pinpoint possibly infected systems more quickly.
- **Take immediate action** and limit the damage that the infection could cause.
- **Calculate an IOC score** (Indication of Compromise) per device.
- **Detect malicious activities** (or attempts to), even if they are prevented by other security solutions.

3.1. Logging in to Web Console

Before accessing the NTSA web console, take into account the following details:

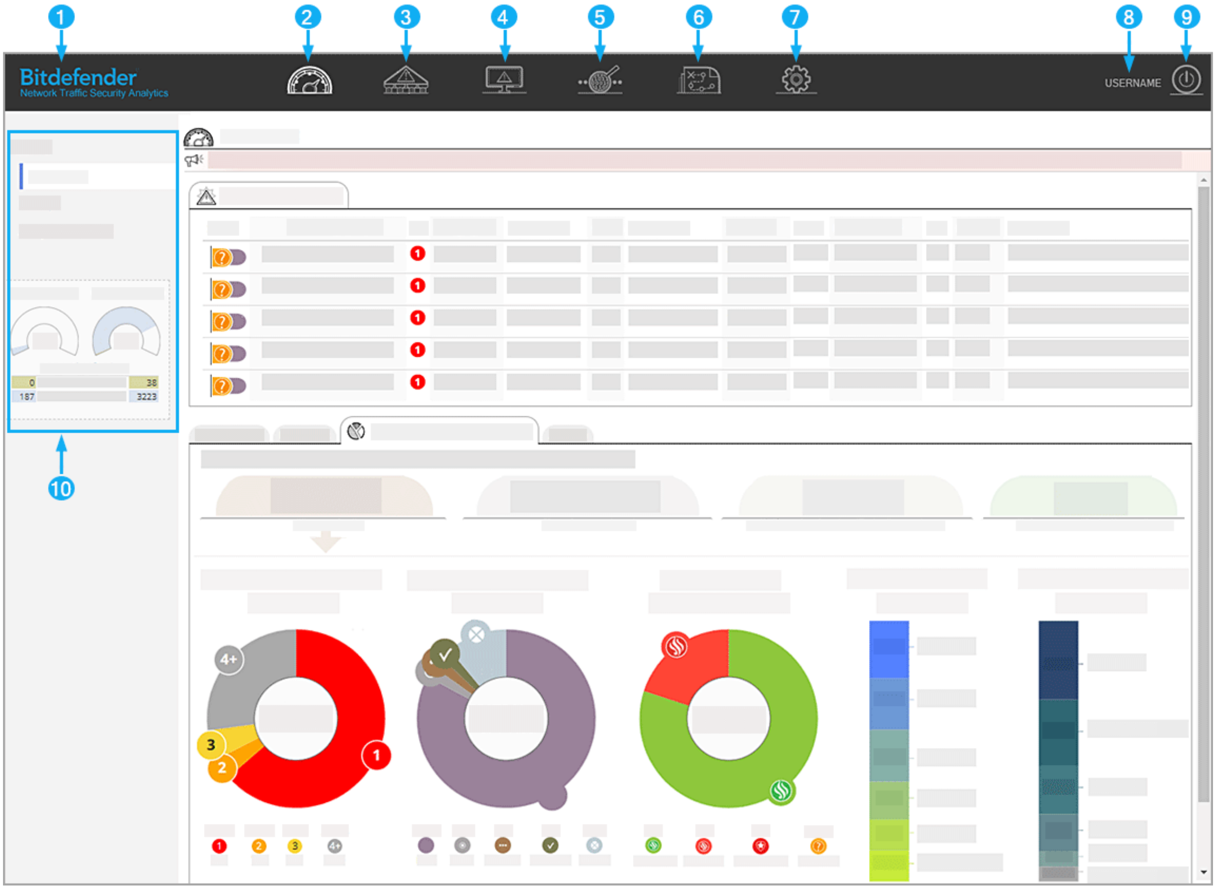
- Make sure you have the web console IP address at hand. To view the web console IP address, access the Bitdefender Network Traffic Security Analyzer TTY console from VMware vSphere Client, where the web console IP address (**eth1**) is being displayed.
- We recommend using Mozilla Firefox or Google Chrome browsers for accessing the NTSA web console. When using any other browser, certain console pages may not display correctly.

To connect to Bitdefender Network Traffic Security Analyzer:

1. Access `https://x.x.x.x` from your browser, where `x.x.x.x` is the web console IP address provided during the Bitdefender Network Traffic Security Analyzer setup.
2. The login page will appear. Enter the default credentials (username: `admin` and password: `bitdefender default`). You can afterwards customize the default password.

After login, the console will display the **Dashboard** page, and you can start monitoring your network.

3.2. NTSA Web Console Overview



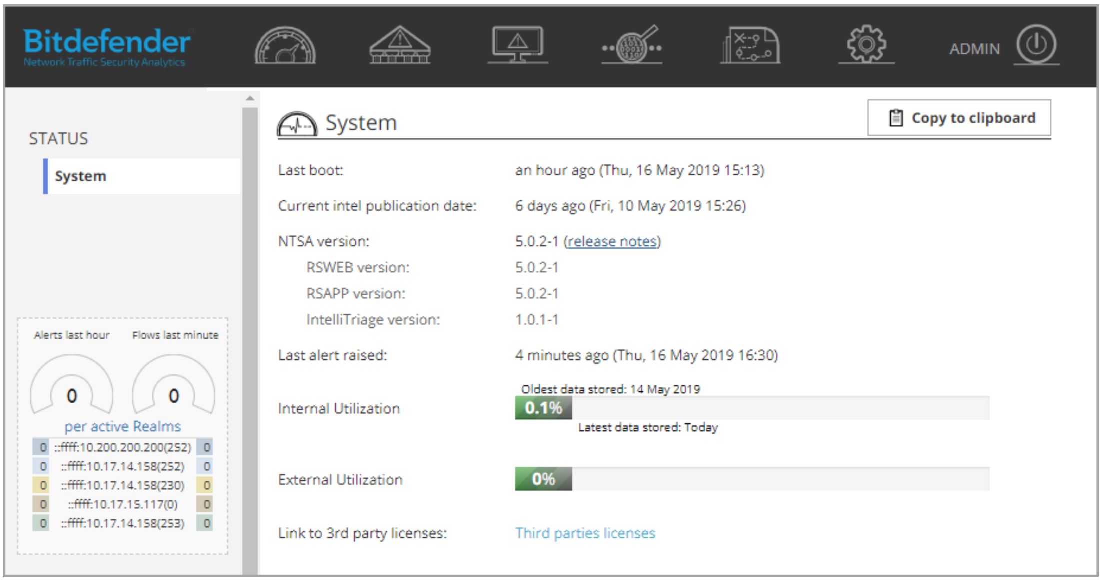
The NTSA Web Console contains several pages, which you can access by clicking the buttons available on the menu bar.

1. System Status
2. Dashboard
3. Alert History
4. Analysis per Device
5. Data Export
6. Logs
7. Settings
8. Logged user name
9. Log in / Log out
10. For each page of the monitoring console, you will notice an information area on the left side panel, displaying your network activity in real-time.

3.2.1. System Status

The system status displays the following information about your NTSA solution:

- The system uptime.
- The last time that the threat intelligence data was being published to the Bitdefender update servers. The system will automatically update itself every hour.
- The current NTSA version number.
- A link to the NTSA release notes web page.
- The status of external and internal storage.
- A link to the License and Services Agreement for Bitdefender NTSA web page.



0	::ffff:10.200.200.200(252)	0
0	::ffff:10.17.14.158(252)	0
0	::ffff:10.17.14.158(230)	0
0	::ffff:10.17.15.117(0)	0
0	::ffff:10.17.14.158(253)	0

Last boot: an hour ago (Thu, 16 May 2019 15:13)

Current intel publication date: 6 days ago (Fri, 10 May 2019 15:26)

NTSA version: 5.0.2-1 (release notes)

RSWEB version: 5.0.2-1

RSAPP version: 5.0.2-1

IntelliTriage version: 1.0.1-1

Last alert raised: 4 minutes ago (Thu, 16 May 2019 16:30)

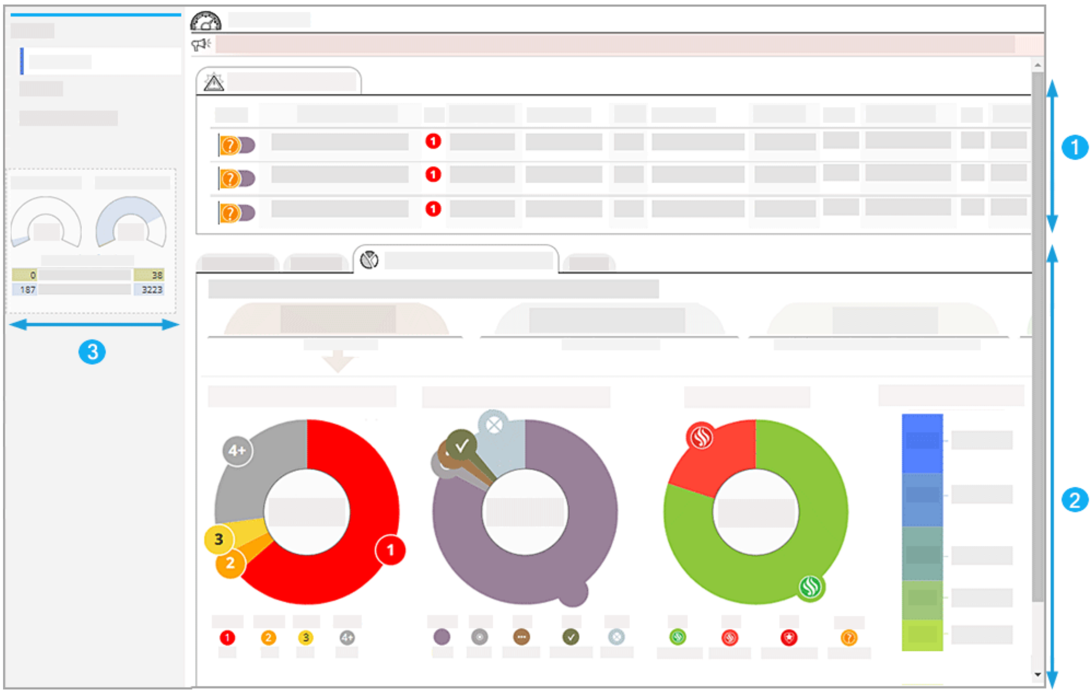
Internal Utilization: Oldest data stored: 14 May 2019 0.1% Latest data stored: Today

External Utilization: 0%

Link to 3rd party licenses: Third parties licenses

3.2.2. Dashboard

This is the default page displayed after login, providing an overview of the active realms, the latest security alerts and network statistics.



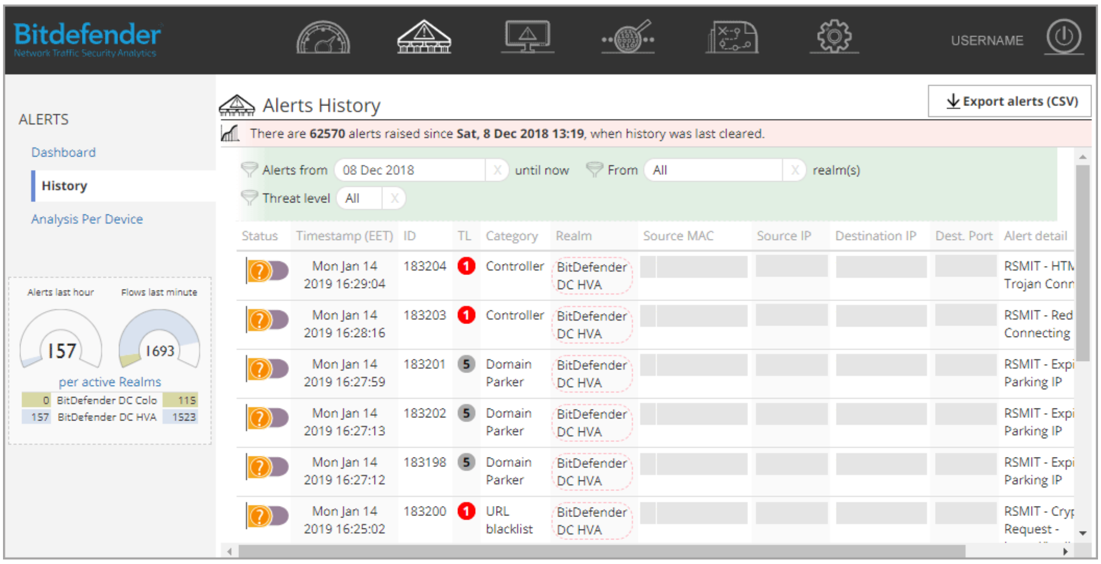
The information provided on this page refers to the following data:

1. Latest Level 1 Alerts: the list with the 10 most recent Threat Level 1(TL1) alerts overall active realms, sorted by time. Click the alert you are interested in to display a page with more details.
2. Alert distribution by time (last 24 hours / last week / last month / all data), including dynamic pie and bar charts. The **Last Month** and **Last 7 Full Days** end the timeframe at 00:00 UTC. Whereas the **Last 24 Hours** and **All Data** tabs do not have a fixed timeframe.
3. The gauges on the left show the distribution of the total amount of alerts and flows by the specified time, along with the associated realm distribution. Click **per Active Realms** to go to the **Realms** page.

You can define all monitoring settings, network configuration and alerts on the **Settings** page.

3.2.3. Alerts History

The alerts history shows you all the available alerts raised since the last date when history was cleared. You can store a maximum of 1.000.000 alerts. To see all the alerts, export the alerts to a CSV file. This can be downloaded with the **export alerts (CSV)** button.



Alerts History

There are **62570** alerts raised since **Sat, 8 Dec 2018 13:19**, when history was last cleared.

Alerts from 08 Dec 2018 until now From All realm(s)

Threat level All

Status	Timestamp (EET)	ID	TL	Category	Realm	Source MAC	Source IP	Destination IP	Dest. Port	Alert detail
?	Mon Jan 14 2019 16:29:04	183204	1	Controller	BitDefender DC HVA	[redacted]	[redacted]	[redacted]	[redacted]	RSMIT - HTM Trojan Conn
?	Mon Jan 14 2019 16:28:16	183203	1	Controller	BitDefender DC HVA	[redacted]	[redacted]	[redacted]	[redacted]	RSMIT - Red Connecting
?	Mon Jan 14 2019 16:27:59	183201	5	Domain Parker	BitDefender DC HVA	[redacted]	[redacted]	[redacted]	[redacted]	RSMIT - Expi Parking IP
?	Mon Jan 14 2019 16:27:13	183202	5	Domain Parker	BitDefender DC HVA	[redacted]	[redacted]	[redacted]	[redacted]	RSMIT - Expi Parking IP
?	Mon Jan 14 2019 16:27:12	183198	5	Domain Parker	BitDefender DC HVA	[redacted]	[redacted]	[redacted]	[redacted]	RSMIT - Expi Parking IP
?	Mon Jan 14 2019 16:25:02	183200	1	URL blacklist	BitDefender DC HVA	[redacted]	[redacted]	[redacted]	[redacted]	RSMIT - Cryp Request -

Alert Status

Alert Qualification

Filtering

Alert Details

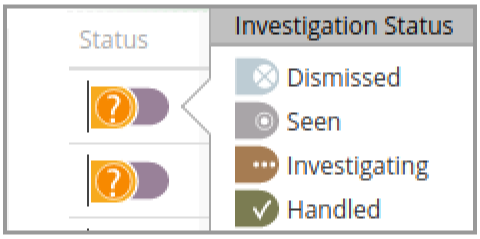
IntelliTriage Details

Flow Data

Alert Status

In the Alert Status, you can set the alert investigation status.

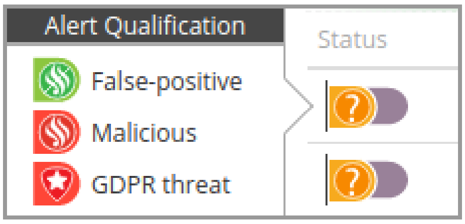
To set an investigation status, click the purple icon and select an option.



Alert Qualification

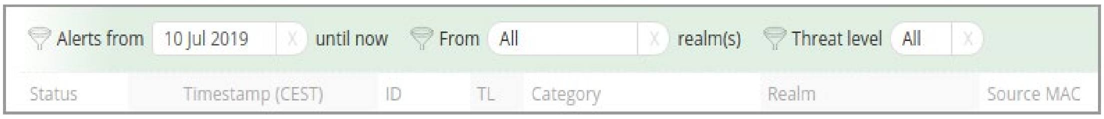
In the Alert Qualification, you can identify and update alerts.

To set an alert status, click the orange question mark icon and select an option. Updated alerts show up in the dashboard as statistics.



Filtering

You can use the filtering option to display specific alerts based on your settings. Your filter is also applied to CSV export files.



Alerts from 10 Jul 2019 until now From All realm(s) Threat level All

Status	Timestamp (CEST)	ID	TL	Category	Realm	Source MAC

Alert Details

In the Alert Details, you can view information such as connection, data source or destination.

To view alert details, click an alert. In the alert panel, you can take the following actions:

- **Copy to clipboard** to copy the information to the clipboard.
- **Look up destination at VirustTotal** to scan it through VirusTotal.
- **Whitelist similar alerts** to whitelist future alerts.

  You can find whitelisted alerts in your custom whitelist.

IntelliTriage Details

In the IntelliTriage Details, you can view an extended level of information and mitigation steps.

To view IntelliTriage information, click an alert and go to the **IntelliTriage Details** tab.

In the IntelliTriage tab, you can take the same actions as for Alert Details.

Flow Data

In Flow Data, you can view the traffic sent by the associated host. Use this information to view outbound data, or packets blocked by your firewall.

To view the flow data, click an alert and click **Show flow data**.

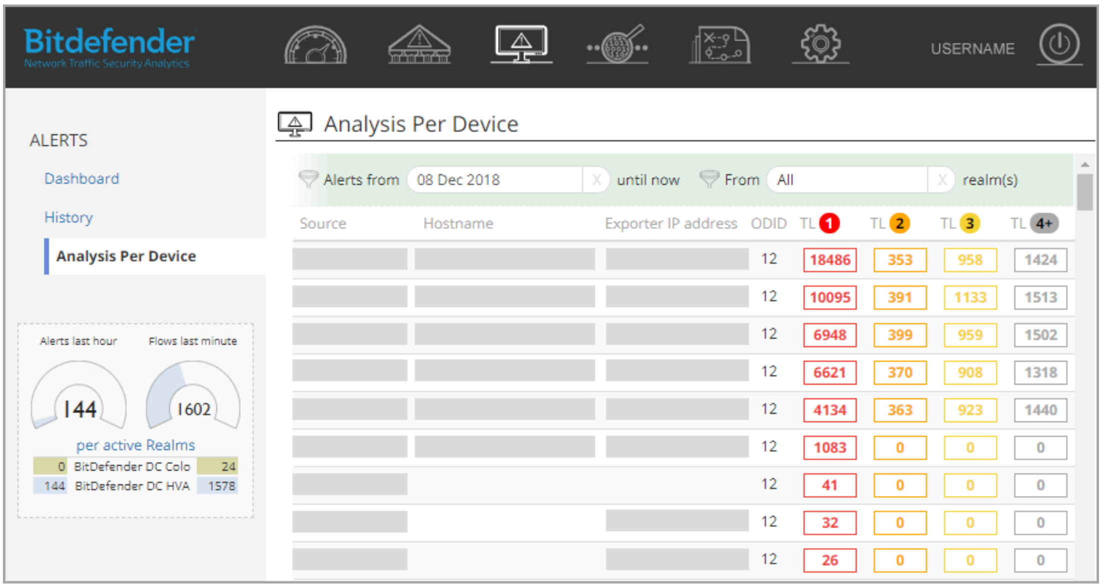
In the flow data, you can take the following action:

- **Export this flow** to export the information to a CSV file.

  This action redirects you the **Flow-Data** page where the CSV file is scheduled for export

3.2.4. Devices

In the Analysis per Device page, you can see all the alerts grouped by source IP address. With this view, you can quickly see which device on your network needs your attention the most. The system that will be displayed on top of this page has the highest IOC score. This score is determined by the number of alerts in combination with the types of alerts. For example, a host with 200 TL2 alerts will end up higher in the ranking than a host with 20 TL1 alerts.



0	BitDefender DC Colo	24
144	BitDefender DC HVA	1578

Analysis Per Device

Alerts from 08 Dec 2018 X until now From All X realm(s)

Source	Hostname	Exporter IP address	ODID	TL 1	TL 2	TL 3	TL 4+
			12	18486	353	958	1424
			12	10095	391	1133	1513
			12	6948	399	959	1502
			12	6621	370	908	1318
			12	4134	363	923	1440
			12	1083	0	0	0
			12	41	0	0	0
			12	32	0	0	0
			12	26	0	0	0

Under the TL columns, you can view the categories that triggered the alerts, on mouse-over.

You can filter the alerts based on date and realms. To view Alert Details, IntelliTriage Details and Flow Data, click a host.

You can set Alert Status and Alert Qualification for the selected host. The alerts will not be deleted, but are greyed out in your view. If new alerts are being raised for this host, the dismissed alerts will be displayed again. The dismissed alerts will not count on the ranking for this host anymore.

3.2.5. Data Export

In the Data Export page, you can export and view flow data for forensic analysis.

- Flow-Data
- Reports
- Events

Flow-Data

In the Flow-Data page, you can view flow data logs and take actions.

To export data:

1. Navigate to **Data Export > Reports**.
2. Click **New data export** at the upper right corner.
3. Configure the following:

- **Export name**. Enter a name for your CSV file.
- **Source IP address**
- **Destination IP address** and **Ports**. Enter a port number or leave the field blank to specify all ports.
- **Realm**. Specify the flow exporter.
- **Storage**
- Select **Internal** to access the flow storage database.
- Select **External** to access external storage database. To configure external storage, navigate to **Settings > Storage**.
- **Date Range**
- **Description**. Add a note to your CSV file.

4. Click **OK**.

To view export details, click an entry in the table. In the details panel, you can take the following actions:

- **CSV_filename.zip** to download the information to a CSV file.
- **Rerun Export** to schedule an export job.

Reports

In the Reports page, you can run and view reports.

To schedule a reporting job:

1. Navigate to **Data Export > Reports**.
2. Click **New report job** at the upper right corner.
3. Configure the following:
   - **Active**
   - **Name**. Enter a name for your report file.
   - **Periodicity**
   - **Time Range**
   - **Recipient**
4. Click **OK**.

   Your report is scheduled to run at midnight. Filters applied to live statistics do not show up in the output file (PDF).

To view report details, click an entry in the table. In the details panel, you can take the following actions:

- **Edit** to modify job details.

- **Instant Download** to download the report as PDF.

Events

In the Events page, you can configure a push notification service to send events to subscribers. A subscriber receives specific events configured by an event publisher. You can configure subscribers as HTTP/HTTPS endpoints, to receive alerts (TL 1 - TL4+), in a SIEM format.

To configure a subscription to receive notifications:

1. Navigate to **Data Export > Reports**.
2. Click **New configuration** at the upper right corner.
3. Configure the following:
    - **Active**. Toggle active state.
    - **Name**. Enter a name for your configured subscription.
    - **URL**. Enter the destination endpoint (HTTP/HTTPS).
    - **Headers**. Enter a key-value pair. Click **+** to add multiple entries.
    - **Type**. Choose **Alert** from the dropdown list and select the Threat Level (**TL**) alerts for which you want to receive notifications.
    - **Realm**. Choose an individual or all realms from the dropdown list.
4. Click **OK** to save the configuration.

    To test the notification service, click the **Send test event** button to send a predefined test event to your configured subscription. You can test subscriptions if you enter the URL.

    To view subscription details, click an entry in the table. In the configuration panel, you can take the following actions:

    - **Edit** to reconfigure a subscription.
    - **Remove** to delete a subscription.

Note
If a connection error occurs at the destination endpoint, the configured subscription will not receive notifications.

3.2.6. Settings

In the Settings page, you can configure the following:

Admin & System

Detection

- Alerting

Admin & System

In the Admin & System page, you can configure the following:

- Users
- Storage
- HTTP Proxy
- Maintenance
- Services
- Network
- SMTP
- Licensing
- Telemetry

Users

In the Users page, you can add new users and learn about the user roles. This page is available to Admins only.

To add a new user:

1. Navigate to **Settings > Admin & System > Users**.
2. Click **Add a new user**.
3. Configure the user information form.
4. Click **OK** to save settings.

   The Admin is prompted with activation details. The new user receives a confirmation email with account activation steps.

Storage

In the **Storage** page, you can view internal data usage and set external storage. The storage is used as a flow storage database. The external storage supports only CIFS and NFS protocols.

To add external storage:

1. Navigate to **Settings > Admin & System > Storage**.
2. Under **Connection Settings,** click the **Edit** button.
3. Configure the connection settings form.
4. Click **OK**.
5. Click the **External storage** slider to activate.

To configure storage settings (advanced use only):

1. Navigate to **Settings > Admin & System > Storage**.
2. Under **Storage Settings,** click the **Edit** button.
3. Configure the following:
   - **User ID (UID)**
   - **Group ID (GID)**
   - **Subdirectory**. This field creates a directory to organize the flow data on the remote server.
   - **Storage quota (GB)**. The default is set to **500**.
   - **Retention time (days)**. The default is set to **365**, after which data flows are deleted.
4. Click **OK** to save settings.

HTTP Proxy

In the **HTTP Proxy** page, you can configure and enable your proxy server.

To configure an HTTP proxy:

1. Navigate to **Settings > Admin & System > HTTP Proxy**.
2. Under **Configuration,** click the **Edit** button.
3. Configure the proxy settings form.
4. Click **OK** to save settings.
5. Click the **Enabled** slider to activate.

Maintenance

In the Maintenance page, you can manage the appliance startup options, clear history or enable remote support.

Services

In the Services page, you can synchronize the time and configure monitoring and event notification settings.

NTP for NTSA ensures the time is synchronized and calibrated for connected probes.

To configure the time server:

1. Navigate to **Settings > Admin & System > Services**.
2. Under **Upstream Time Servers - NTP for NTSA,** click the **Edit** button.
3. Add your time server.

4. Click **+** to add multiple time servers.
5. Click **OK**.

SNMP reports server statistics such as disk utilization, network traffic and server performance counters.

To configure SNMP:

1. Navigate to **Settings > Admin & System > Services**.
2. Under **SNMP Configuration,** click the **Edit** button.
3. In the **Enabled** click **None** and choose from the following versions:
    - **v2**. This version requires a plaintext community string (passphrase).
    - **v3.** This version adds both encryption and authentication.
4. Click **OK**.

Network

In the Network page, you can set up NTSA networking information, if needed. NTSA uses DHCP and does not require IP assignment but you can configure this if your network does not support it.

To configure NTSA networking information:

1. Navigate to **Settings > Admin & System > Network**.
2. Under **Internet and Flow Data,** click the **Edit** button.
3. Configure the settings to provide access to NTSA.
4. Click **OK** to save settings.

SMTP

In the SMTP page, you can configure your internal mail relay settings to receive email notifications, if needed.

To configure internal mail relay:

1. Navigate to **Settings > Admin & System > SMTP**.
2. Under **SMTP,** click the **Edit** button.
3. Configure your mail server settings.
4. In the **System recipient(s)** field, enter the recipient’s email address.
5. Click **+** to add multiple recipients.
6. Click **OK** to save settings.

To test the internal mail relay, click the **Send test message** button.

Licensing

In the Licensing page, you can configure your NTSA license. Choose from the following licensing modes:

- Standalone (via license key)
- Bitdefender GravityZone integration (via token)

To license your NTSA as a standalone product:

1. Navigate to **Settings > Admin & System > Licensing**.
2. Click the **Standalone or Integration with GravityZone** edit button.
3. Select **Standalone** and enter your license key.
4. Click **OK**.

To license your NTSA through GravityZone integration:

1. Navigate to **Settings > Admin & System > Licensing**.
2. Click the **Standalone or Integration with GravityZone** edit button.
3. Select **Integration with GravityZone** and click **Generate an Integration Token**.
4. Click **Copy to clipboard** to save the value.
5. Open GravityZone Control Center.
6. Navigate to **Configuration > NTSA**.
7. Select the **Integration with Network Traffic Security Analytics (NTSA)** checkbox to complete the integration.
8. Enter your hostname or IP address.
9. In the **Token** field, paste the value.
10. Click **Save** to save settings.

Telemetry

In the Telemetry page, you can enable anonymous usage statistics, such as running version and active license type. The information is sent to Bitdefender on an hourly basis.

Detection

In the Detection page, you can configure the following:

Categories

Whitelist

Blacklist

Categories

In the Categories page, you can configure the alert categories. The list of alert categories consists of indicators of compromise (IOCs). You can check/uncheck the categories according to the associated threat level.

Whitelist

In the Whitelist page, you can allow matching traffic from source IP addresses to destination IP addresses. Whitelisted items do no generate alerts.

To whitelist an item:

1. Navigate to **Settings > Detection > Whitelist**.
2. Click the **Configuration** button.
3. Click **+** to add a new item.
4. Configure the following:
    - **Enabled**. Select the checkbox to enable.
    - **Protocol**. Select from the dropdown list.
    - **Category**. Select a category from the dropdown list. To include a category, add at least one other configuration criterion. To whitelist an entire category, go to the **Categories** page.
    - **Description**. Add a description to your item.
5. Click **OK** to save changes.

To remove an item from the whitelist:

1. Navigate to **Settings > Detection > Whitelist**.
2. Click the **Configuration** button.
3. Click the remove button.

You can choose to import or export whitelists as JSON files. Use the **Import list** and **Export list** buttons at the upper right corner to perform these operations.

Blacklist

In the **Blacklist** page, you can add specific IP addresses for which to receive alerts.

To blacklist an IP address:

1. Navigate to **Settings > Detection > Blacklist**.
2. Click the **Configuration** button.
3. Click **+** to add a new item.
4. Configure blacklist settings.

5. Click **OK** to save changes.

To remove an IP address from the blacklist:

1. Navigate to **Settings > Detection > Blacklist**.
2. Click the **Configuration** button.
3. Click the remove button.

You can choose to import or export blacklists as JSON files. Use the **Import list** and **Export list** buttons at the upper right corner to perform these operations.

Alerting

In the Alerting page, you can configure the following:

IP/Mac Aliases

Realms

E-Mail

Syslog

IP/MAC Aliases

In the IP/MAC Aliases page, you can create alias names for your IP or MAC addresses. IP/MAC alias names provide better visibility in the Alerts History page.

To create an IP/MAC alias:

1. Navigate to **Settings > Alerting > IP/MAC Aliases**.
2. Click the **Configuration** button.
3. Add you IPv4 or MAC address.
4. Enter an alias name.
5. Click **OK** to save settings.

Realms

In the Realms page, you can create alias names for your realms. A realm identifies the data flow source, linking together the exporter IP address to the Observation Domain ID (ODID). Realm alias names provide better visibility in the Alerts History page.

To create a realm alias:

1. Navigate to **Settings > Alerting > Realms**.
2. Click the **Activation and Aliases** edit button.

3. Enter a name under the **Alias** field.
4. Select the **Active** checkbox if you want to receive alerts and trigger alerts for the specified realm.

   Muted realms are not included in statistics and are unavailable for alert filtering.
5. Click **OK** to save settings.

E-Mail

In the E-mail page, you can configure alert preferences to receive email notifications.

To configure email notifications:

1. Navigate to **Settings > Alerting > SMTP**.
2. Click the **Notifications** edit button.
3. In the **Alert recipient(s)** field, enter the recipient's email address.
4. Click **+** to add multiple recipients.
5. Choose the alert threat level.
6. Click **OK** to save settings.

Syslog

You can configure NTSA to forward alerts to an external Syslog or Security Information and Event Management (SIEM) server. All events are forwarded in cleartext. The content and format of the log messages are according to the chosen format.

NTSA will still record all alerts and display them in reports and graphs in the NTSA web console if you enable event forwarding to a Syslog or SIEM server.

To configure the alerts forwarding to a Syslog or SIEM server:

1. Navigate to **Settings > Alerting > Syslog**.
2. Enable sending alerts to Syslog.
3. Click the configuration icon next to Syslog and edit the settings:
   - **Server**: the Hostname or IP address to which events should be sent. The Syslog or SIEM server and any routers, firewalls and security groups must allow inbound connections from NTSA for event forwarding to work.
   - **Port**: usually port 514, but it can be different according to the settings in your infrastructure.
   - **Transport**: Choose between UDP and TCP as the transport protocol.
4. Click the configuration icon next to NOTIFICATIONS to edit the settings:
   - **Format**:-select the appropriate format (RedSocks or Common Event Format), according to the integration that you want.
   - **Threat level(s)** – Select individual or multiple threat levels.
5. Click **OK** to save the settings.

You can test the Syslog configuration by clicking the **Send test message** button, which will send a test message to the configured server.

Response

In the Response page, you can integrate NTSA with Bitdefender GravityZone and configure automated actions, based on unusual activity reported by the Probes.

Actions

Integrations

Actions

In the **Actions** page, you can configure automated actions through the Bitdefender GravityZone integration. You can configure the automated actions to trigger a specific scan task when an alert category is identified. These actions will also trigger notifications in Control Center. To configure automated actions, you must first configure the integration.

To configure automated actions:

1. Navigate to **Settings > Response > Actions**.
2. Click the **+** to add a new entry.
3. Configure the following:
   a. **Name**. Enter a name for the automated action.
   b. **Alert Category**. Choose an alert category from the dropdown list. You can only choose TL 1 Categories.
   c. **Integration**. Choose the GravityZone integration from the dropdown list.
   d. **Scan Task**. Choose a scan task from the dropdown list.
      - **Quick Scan**. This option uses in-the-cloud scanning to detect malware running in the system.
      - **Full Scan**. This option scans the entire system for all types of malware threatening its security, such as viruses, spyware, adware, rootkits and others
      - **Memory Scan**. This options checks for any programs running in the endpoint's memory.
4. Click **OK** to save settings.

   To view scan results, open Control Center and go to the **Tasks** page. For more information about scan tasks, refer to the GravityZone Administrator's Guide.

Integrations

In the Integrations page, you can integrate NTSA with Bitdefender GravityZone. The integration is done via APIs and the communication is established through HTTPS.

To configure the integration, follow these steps:

1. Generate API Key in Control Center
2. Configure integration in NTSA

Generate API Key in Control Center

1. Log in to GravityZone Control Center.
2. Click the username at the upper-right corner and choose **My Account**.
3. Go to the API keys section and click **Add** at the top side of the table.
4. Enable your APIs.

   You must include at least **Network API** to establish communication with NTSA.
5. Click **Save**.

   An API key is generated. To prevent the leaking of sensitive information, do not share or distribute your own generated API keys.
6. Copy the Access URL from the Control Center API section.

   Continue configuring the integration in the NSTA Web Console.

Configure integration in NTSA

1. Log in to NTSA Web Console.
2. Navigate to **Settings > Response > Integrations**.
3. Click **+** to add a new entry.
4. Configure the following:
   - **Name**. Enter a name for the integration.
   - **Type**. Choose the GravityZone service type.
   - **IP/FQDN**. Enter the Control Center hostname.

     For GravityZone Cloud, you can have multiple integrations using the same IP/FQDN. For GravityZone On-Premises, the IP/FQDN must be unique, allowing for a single integration only.
   - **Port**. Enter a port number.
   - **Authentication**. Enter the API key, generated in Control Center
5. Click **OK** to complete the integration.

   You can view the integration status under the **Status** column. The following status information is available:
   - **Connected** for successful integrations.
   - **Invalid** for unsuccessful integrations.
   - **Pending** for current integration approval processes.

A. Appendix

A.1. Glossary of Terms

IPFIX (Internet Protocol Flow Information Export)

An IETF protocol allowing network engineers and administrators to collect flow information from routers, probes and other switches then analyze the flow data through a network analyzer. The IPFIX standard defines how IP flow information is to be formatted and transferred from an exporter to a collector.

Egress

Data egress refers to data leaving a network in transit to an external location. Examples of common channels for data egress include email, web uploads, cloud storage, removable media (USB, CD/DVD or external hard drives), FTP/HTTP transfers.

STIX and TAXII

STIX (Structured Threat Information Expression) and TAXII (Trusted Automated Exchange of Indicator Information) represent standards aimed to improve the prevention and mitigation of cyber-attacks. These standards are not pieces of software themselves, but rather specifications that software can use. The combination of STIX and TAXII allow sharing more easily threat information with your constituency and peers.