

## Integration Guide: SonicOS and Fastvue Reporter

May 2019

This document describes how SonicOS is integrated with Fastvue Reporter. Such integration allows Fastvue Reporter to interpret SonicWall firewall log files giving real-time web activity reports. It also integrates with SonicWall's Content Filtering System (CFS) and its authentication tools for security and protection.

### Topics:

- [About Fastvue](#)
- [Requirements](#)
- [Installing Fastvue Reporter](#)
- [Configuring Your SonicWall Syslog](#)
- [References](#)

## About Fastvue

**Fastvue** helps businesses and schools deliver useful Internet usage reports to human resources personnel, teachers, department managers and information technology staff. You can use Fastvue Reporter for SonicWall to:

- Send scheduled reports to department managers and HR detailing their staff's Internet usage.
- Safeguard students by monitoring access to self-harm, extremist, or inappropriate content.
- Monitor and troubleshoot your network in real-time to uncover the firewall features and policies responsible for allowing or blocking specific traffic.

## Requirements

- Fastvue Reporter
- SonicOS 6.2.6 and above, SonicOS 5.8/5.9
- Windows Server 2008 R2 and above (x64 Windows Operating Systems)
- .NET 4.6, Microsoft IIS, Open JDK and Elasticsearch are automatically installed and configured
- Minimum CPU and RAM recommendations: Less than 500 users - 4 CPUs/Cores, 6 GB RAM

## Installing Fastvue Reporter

- 1 Go to <https://www.fastvue.co/sonicwall/> and click **DOWNLOAD**.
- 2 In the **Download Fastvue Reporter for SonicWall** popup window enter your contact details, and click **DOWNLOAD** again.

- 3 Install **Fastvue Reporter for SonicWall** on a machine (or virtual machine) that meets the recommended requirements for your network size.

**i** | **NOTE:** Installing Fastvue Reporter for SonicWall also installs and configures .NET 4.6, Microsoft IIS, and Open JDK and Elasticsearch.



## Configuring Your SonicWall Syslog

Configure SonicWall to send network and web traffic events via Syslog to the Fastvue Reporter machine.

- 1 Go to **MANAGE | Logs & Reporting | Log Settings | SYSLOG**.
- 2 Under **Syslog Settings**, set the **Syslog Format** to **Enhanced Syslog** from the drop-down list.

- 3 Click **ACCEPT** to apply the settings to all Syslog Servers except for GMS and Analyzer.
- 4 Click the **Enhanced Syslog Fields Settings** button to the right and check all the available fields.

**Enhanced Syslog Settings**

**General**

Host (sn)       Event ID (m)       Category (cat)       Group Category (gcat)

Message (msg)

**Interface**

Src Interface       Src Mac Addr (srcMac)       Dst Interface       Dst Mac Addr (dstMac)

**Protocol**

Src IP (src)       Src NAT IP (natSrc)       Src Port       Src NAT Port

Dst IP (dst)       Dst NAT IP (natDst)       Dst Port       Dst NAT Port

Protocol (proto)       ICMP type (type)       ICMP code (icmpCode)

**Connection**

Bytes Rcvd (rcvd)       Bytes Sent (sent)       Pkts Rcvd (rpkt)       Pkts Sent (spkt)

User (usr)       Conn Duration (cdur)       Session Type (sess)       Session Time (dur)

Src VPN Policy (vpnpolicy)       Dst VPN Policy (vpnpolicyDst)       Src Zone (srcZone)       Dst Zone (dstZone)

Client Policy (rule)       Interface stats       SonicPoint Stats

**Application**

HTTP OP (op)       HTTP result (result)       URL (dstname)       Block Reason (code)

Application (app)       GMS Heartbeat       GMS change URL (Change)

**Others**

Counter (n)       NPCS (npcs)       Note (note)       IDP

Anti Spam       App Firewall       Raw Data       File ID

File Tx Status       Rule Action (fw\_action)       uid

- 5 Click **SAVE**.
- 6 Under **Syslog Servers**, click **ADD** to add your Fastvue Reporter server.

**Syslog Servers**              to 0 (of 0)   

#	Event Prof...	Server Name	Server P...	Server Type	Server Facility	Server Format	Server ID	Enable	Con...
No Entries									

- 7 In the popup dialog window that displays, choose **Select an address object** next to **Name or IP Address**.

SONICWALL™ NS<sub>a</sub> 9650

Event Profile:

Name or IP Address:

Port:

Server Type:

Syslog Format:

Syslog Facility:

Syslog ID:

Enable Event Rate Limiting  
Maximum Events Per Second:

Enable Data Rate Limiting  
Maximum Bytes Per Second:

Bind to VPN Tunnel and Create Network Monitor Policy in NDPP Mode:

Local Interface:

Outbound Interface:

**Ready**

- 8 In the popup dialog window that displays, enter the **Name**, **Zone Assignment**, **Type**, and **IP Address** of your Fastvue Reporter server.
- 9 Click **OK** when done.

SONICWALL™ NS<sub>a</sub> 9650

Event Profile:

Name or IP Address:

Port:

Server Type:

Syslog Format:

Syslog Facility:

Syslog ID:

Enable Event Rate Limiting  
Maximum Events Per Second:

**Add Address Object - Google Chrome**

**SONICWALL™ NS<sub>a</sub> 9650**

Name:

Zone Assignment:

Type:

IP Address:

**Ready**

After this step you see the Fastvue Reporter IP Address listed under the **Server Name** column of the **Syslog Servers** section.

- 10 Go to **MANAGE | Logs & Reporting | Log Settings > Base Setup**.
- 11 Under the **Category** column, expand the **Log > Syslog** section.
- 12 Under the **Syslog** section, check the **Syslog Website Accessed** events.
- 13 Check the Syslog box, in the **Syslog Website Accessed** row, and ensure the **Priority** is set to **Inform**.
- 14 In the **Event Count** column, check to see if the number of **Syslog Website Accessed** events are increasing. If not, ensure **Content Filtering Services** is licensed and configured.

Category	Color	ID	Priority	Gui	Alert	Syslog	Ipfix	Email	Event Count
System			Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1698
Log			Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
FTP			Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Configuration Auditing			Inform	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Syslog			Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Syslog Server Unreachable	■	657	Inform	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Maximum Syslog Data Rate Exceeded	■	655	Critical	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Syslog Website Accessed	■	97	Inform	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
E-mail			Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
General			Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1
Security Services			Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	39
Users			Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	443
Firewall Settings			Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	42201
Network			Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1214273
VPN			Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
High Availability			Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
3G/4G, Modem, and Module			Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
Firewall			Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
Wireless			Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0

Dropped by Reason:

- Overflow 0
- GUI Filter 0
- Alert Filter 0
- Syslog Filter 0
- IPFIX Filter 0
- E-mail Filter 0
- Priority 0
- Syslog Event Rate 0
- Syslog Data Rate 0

- 15 In the **Category** column, expand **Network** and check the **Syslog** boxes for **Connection Closed**, **Web Request Receiver**, and **Web Request Drop**, and ensure the Priority is set to **Inform**.
- 16 In the **Category** column, expand **Security Services** and check the **Syslog** boxes for **Website Accessed**, and **Website Blocked**, and ensure the Priority is set to **Inform**.
- 17 Check the **Syslog** boxes for the **Website Accessed** and **Website Blocked** rows.
- 18 Click **ACCEPT**.

Category	Color	ID	Priority	Gui	Alert	Syslog	Ipfix	Email	Event Count
▶ FTP	<input type="checkbox"/>		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
▶ Configuration Auditing	<input type="checkbox"/>		Inform	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
▼ Syslog	<input type="checkbox"/>		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
Syslog Server Unreachable	<input checked="" type="checkbox"/>	657	Inform	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
Maximum Syslog Data Rate Exceeded	<input checked="" type="checkbox"/>	655	Critical	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0
Syslog Website Accessed	<input checked="" type="checkbox"/>	97	Inform	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
▶ E-mail	<input type="checkbox"/>		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
▶ General	<input type="checkbox"/>		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1
▶ Security Services	<input type="checkbox"/>		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	45
▶ Users	<input type="checkbox"/>		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	29
▶ Firewall Settings	<input type="checkbox"/>		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	41841
▶ Network	<input type="checkbox"/>		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1158004
▶ VPN	<input type="checkbox"/>		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
▶ High Availability	<input type="checkbox"/>		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
▶ 3G/4G, Modem, and Module	<input type="checkbox"/>		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
▶ Firewall	<input type="checkbox"/>		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
▶ Wireless	<input type="checkbox"/>		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
▶ VoIP	<input type="checkbox"/>		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
▶ SSL VPN	<input checked="" type="checkbox"/>		Inform	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
▶ Anti-Spam	<input type="checkbox"/>		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	320
▶ WAN Acceleration	<input type="checkbox"/>		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
▶ SD-WAN	<input type="checkbox"/>		Mixed	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	3

ACCEPT CANCEL

19 Go to **MANAGE | Security Configuration | Security Services > Content Filter**.

20 Choose **SonicWall CFS**, from the drop-down choices, next to **Content Filter Type**.

21 Under **Global Settings**, check **Enable Content Filtering Service**.

Content Filter Type:

**CFS Status**

License Status: Activated  
 Expiration Date: 04/17/2020  
 Server Status: Server is ready

**Global Settings**

Max URL Caches (entries):   
 Enable Content Filtering Service  
 Block if CFS Server is Unavailable  
 Server Timeout:  second(s)  
 Enable Local CFS Server  
 Primary Local CFS Server:   
 Secondary Local CFS Server:

**CFS Exclusion**

Exclude Administrator  
 Excluded Address:

**CFS Custom Category**

Enable CFS Custom Category

ADD DELETE EXPORT IMPORT

Lookup Domains Containing String:  DELETE ALL

#	Domain	Categories	Configure
No Entries			

ADD DELETE EXPORT IMPORT DELETE ALL

ACCEPT CANCEL

22 Click **ADD** and then click **ACCEPT**.

**Create a CFS policy for your LAN network or zone:**

In the CFS Policy dialog box, enter the following from the drop-down choices:

- **Name**
- **Source Zone**
- **Destination Zone**
- **Source Address Included**
- **Source Address Excluded**
- **User/Group Included**
- **User/Group Excluded**
- **Schedule**
- **Profile**
- **Action**

**i** **NOTE:** Report quality improves when using the following SonicWall features:

- Enabling CFS
- Enabling Authentication
- Enabling DPI-SSL (Decryption Services)
- Enabling Name Resolution
- Logging Referrer URLs
- Blocking QUIC

## Add Your SonicWall as a Source in Fastvue Reporter

- 1 Add SonicWall as a Source in Fastvue Reporter on the Start Page after your installation, or in the top navigation section of Fastvue Reporter in **Settings | Sources | Add Source**.
- 2 Enter the **SonicWall Host or IP** address and **Syslog Port** in the fields provided.
- 3 Click **Add Source** or **Let's Go** on the **Start Page**.

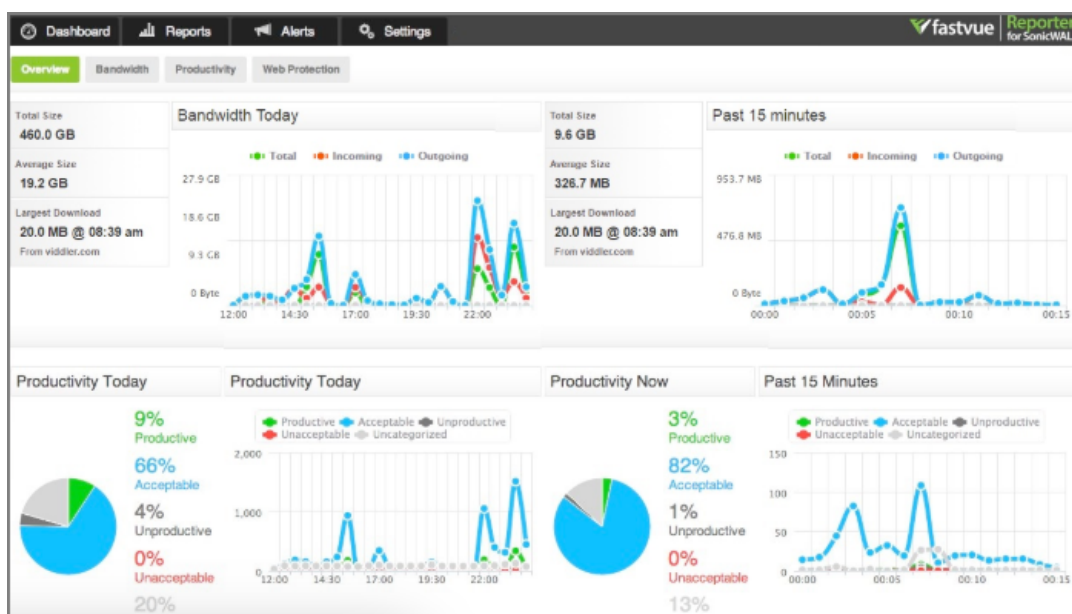


The screenshot shows a web browser window titled "fastvue Reporter for SonicWALL". The main heading is "Add a SonicWALL Source". Below the heading, there is a small instruction: "Ensure SonicWALL is sending syslog messages to the Fastvue Reporter for SonicWALL Server. Then add the SonicWALL as a source below." There are two input fields: "SonicWALL Host or IP" with the value "192.168.1.100" and "Syslog Port" with the value "514". Below these fields is a button labeled "Add Source".

**i** **NOTE:** Ensure SonicWall is sending syslog messages to the Fastvue Reporter from the SonicWall server. Then add the SonicWall as a source.

# Explore Fastvue Reporter for SonicWall

- 1 Go to **Dashboard | Overview** to see the **Bandwidth Today**, **Productivity Today**, **Productivity Now**, and **Past 15 minutes** charts.
- 2 Go to **Dashboard | Overview** to choose from the three Fastvue dashboards in the top navigation menu: **Bandwidth**, **Productivity**, and **Web Protection**.
- 3 Go to the **Reports**, **Alerts**, and **Settings** pages in the top navigation for more services.



- 4 Under **Reports**, choose between **Overview Report**, **User Overview Report** and **Activity Report**.

The screenshot shows the Fastvue Reporter Reports page. The 'Overview Report' tab is selected. The report configuration area shows three criteria:

- 1 Security Group (Contains Admins)
- 2 Source IP (In subnet 192.168.1.0/24)
- 3 Site Domain (Equal to Enter Site Domains)

A dropdown menu is open for Site Domain, showing options like Site Resource, Site Query, Site Country, URL, and URL with Query.

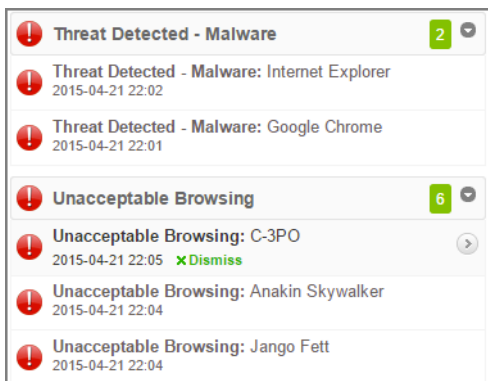
- 5 Under **Activity Report**, see the **Start Time**, **End Time**, **Browsing Time**, and **Origin Domain** of your activity.



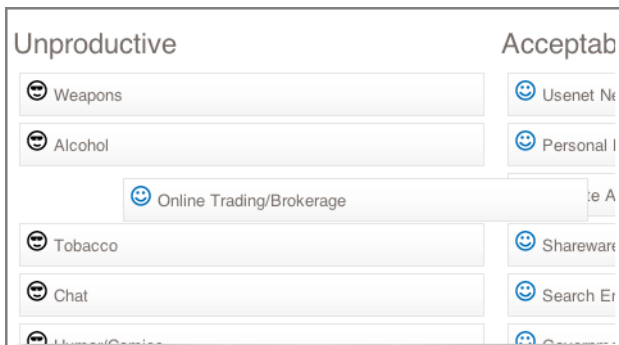
20:00

Start Time	End Time	Browsing Time	Origin Domain
▶ 20:02:35	20:59:43	00:12:37	google.com
▶ 20:21:48	20:52:35	00:01:04	producthunt.com
▶ 20:22:05	20:47:07	00:08:37	facebook.com
▶ 20:25:41	20:47:07	00:06:02	workable.com
▶ 20:25:46	20:31:12	00:05:26	github.com
▶ 20:32:11	20:40:40	00:03:28	invisionapp.com
▶ 20:35:37	20:45:40	00:00:00	wistia.net
▶ 20:40:17	20:42:39	00:02:22	applicantpro.com
▶ 20:42:56	20:46:42	00:03:46	youtube.com
▶ 20:52:23	20:58:05	00:00:31	retentiontab.com
▶ 20:52:41	20:54:02	00:01:21	weworkremotely.com

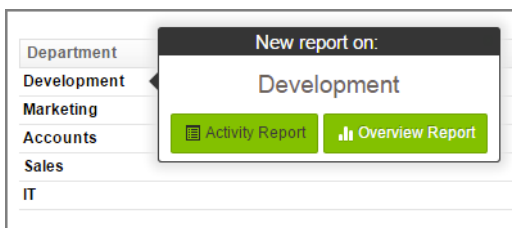
- 6 Under **Alerts**, choose categories such as **Threat Detected - Malware** or **Unacceptable Browsing** to receive instant notifications regarding your security concerns.



- 7 Under **Settings | Productivity Reporting**, adjust your organization's web productivity by dragging and dropping SonicWall's URL categories onto the desired list such as **Unproductive** or **Unacceptable Browsing**.



- 8 Share your Fastvue reports with others using **Scheduled Reports** or by clicking the **Share** button at the top of each report.



- 9 Configure all your SonicWall devices to send Syslog messages to Fastvue Reporter to achieve centralized reporting.



10 Go to **Settings | Data Storage** to see your data usage.

11 Go to **Settings | Data Storage | Settings** to set your **Data Retention Policy** and how large Fastvue Reporter should be for SonicWall's log database.

Category	Color	ID	Priority	Gui	Alert	Syslog	Ipfix	Email	Event Count	
▶ FTP	<input type="checkbox"/>		Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	0	
▶ Configuration Auditing	<input type="checkbox"/>		Inform	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	0	
▼ Syslog	<input type="checkbox"/>		Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	0	
Syslog Server Unreachable	<input checked="" type="checkbox"/>	657	Inform	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0	
Maximum Syslog Data Rate Exceeded	<input checked="" type="checkbox"/>	655	Critical	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	0	
Syslog Website Accessed	<input checked="" type="checkbox"/>	97	Inform	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	
▶ E-mail	<input type="checkbox"/>		Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	0	
▶ General	<input type="checkbox"/>		Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	1	
▶ Security Services	<input type="checkbox"/>		Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	45	
▶ Users	<input type="checkbox"/>		Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	29	
▶ Firewall Settings	<input type="checkbox"/>		Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	41841	
▶ Network	<input type="checkbox"/>		Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	1158004	
▶ VPN	<input type="checkbox"/>		Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	0	
▶ High Availability	<input type="checkbox"/>		Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	0	
▶ 3G/4G, Modem, and Module	<input type="checkbox"/>		Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	0	
▶ Firewall	<input type="checkbox"/>		Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	0	
▶ Wireless	<input type="checkbox"/>		Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	0	
▶ VoIP	<input type="checkbox"/>		Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	0	
▶ SSL VPN	<input checked="" type="checkbox"/>		Inform	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	0	
▶ Anti-Spam	<input type="checkbox"/>		Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	320	
▶ WAN Acceleration	<input type="checkbox"/>		Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	0	
▶ SD-WAN	<input type="checkbox"/>		Mixed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	3	

## References

For more information on using Fastvue Reporter for SonicWall, go to <https://www.fastvue.co/sonicwall>, or contact Fastvue at <https://www.fastvue.co/support>.

## Copyright © 2019 SonicWall Inc. All rights reserved.

This product is protected by U.S. and international copyright and intellectual property laws. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.


The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserve the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.


For more information, visit <https://www.sonicwall.com/legal>.

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/legal/eupa>.

## Legend

 **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

 **IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Last updated: 5/17/19