# Release Notes

Management and Reporting

**Dell SonicWALL Scrutinizer 11.5.2 Release Notes**

## Contents

*Scrutinizer Product Overview* ..... *1*
*System Requirements* ..... *10*
*New Features in Scrutinizer 11.5.2* ..... *11*
*Resolved Issues* ..... *11*
*How to Upgrade to the Licensed Version* ..... *13*
*FAQ* ..... *14*
*Related Technical Documentation* ..... *19*

## Scrutinizer Product Overview

Dell SonicWALL Scrutinizer is a network traffic monitoring, analysis and reporting tool. Scrutinizer is a mature and feature rich flow analytic platform.

Scrutinizer is used to monitor the overall health of the network, troubleshoot irregular network traffic patterns and optimize network performance. The Scrutinizer application is run on a Windows server and accessible through a web-based Graphical User Interface (GUI). IT administrators use Dell SonicWALL Scrutinizer to collect, monitor, and analyze data on user and application usage across the network. Scrutinizer provides administrators with great insight into *how* the network is being used through the use of highly customized granular reporting. Administrators can be alerted based upon a set threshold or on a pre-determined schedule.

Scrutinizer supports a wide variety of flow protocols allowing compatibility with virtually every collector available in the market today. In addition to Dell SonicWALL's pioneering IPFIX implementation in SonicOS 5.8+, Scrutinizer also supports Cisco's Flexible NetFlow. Customers utilizing Scrutinizer receive even greater value for their investment as the software can be utilized to monitor an ever increasing number of switches and routers, due to support for numerous additional industry standards such as NetFlow v5, NetFlow v9, sFlow and J-Flow. Additional supported hardware vendors include Enterasys, Foundry, Juniper, Riverbed, VMware, Citrix, ADTRAN, Nortel and many others.

Supporting a broad range of network devices, flow protocols, and application types, Scrutinizer is flexible enough to be utilized on virtually any network. Administrators are able to leverage reports to reach a level of visibility previously not possible. The network mapping feature allows administrators visibility into almost every link on the network greatly enhancing troubleshooting efforts. Scrutinizer's powerful analytics engine provides users with in-depth traffic analysis which was previously only available through packet-based instrumentation. Advanced analysis algorithms and premier industry usage of IPFIX and NBAR based technologies are at the core of Scrutinizer's impressive set of application level reporting and alerting capabilities.

Scrutinizer is a free tool for download by any IT professional. Three of the main limitations of the free product are that it:

- Only stores a maximum of 24 hours of data
- Does not include most Dell SonicWALL specific reports
- Can only support up to five devices

For the first 30 days after installation, the free Scrutinizer product includes the Flow Analytics Module. To make use of the features available in the Flow Analytics Module beyond the first 30 days, you have to purchase and activate a Flow Analytics Module license.

There are three optional add-on modules for Scrutinizer which are sold separately: the Flow Analytics Module, the Multi-Tenancy Module, and the Advanced Reporting Module.

## *Scrutinizer Base Product*

The base Scrutinizer product includes many great features such as:

### Administration

- Customizable Dashboards
- Group Based User Permissions
- Unique Dashboards per login

With Scrutinizer's suite of built-in administrative tools, customizing specific user logins and dashboards is a breeze. Administrators can create specific permissions based upon a particular user identity or create group based user permissions for entire departments. The Dashboard can be customized on a per-user basis to provide the information that is most relevant to each user.

### Alerting

- Support for on-demand email reporting
- Ability to batch schedule and email reports to administrators

Scrutinizer was built with ease of use in mind. With Scrutinizer's alerting features administrators have "set it and forget it" flexibility when it comes to reporting. Reports can be run based upon a specific schedule or triggered when event thresholds are exceeded. Once configured, reports can be automatically batched and emailed to administrator in several formats.

### Flexible Reporting

- In the Free version, data can be archived for up to 24 hours. Data can be saved longer if a commercial version is purchased.
- Extensive Flexible NetFlow template support
- Granularly defined reports down to the second which can include / exclude data filters
- Create and save templates to easily reuse for future reporting
- Create application group reports based upon specific ports or subnets
- Display data by number of bits, bytes, packets or as a percentage of total traffic
- Per interface, host, protocol, application, or conversation reporting
- Trend data in, out, or bi-directionally

Granular, flexible reporting is the heart of the Scrutinizer product. Administrators have endless possibilities for generating reports based upon general or very specific criteria. Want to know which users are consuming the most bandwidth? Would you like that done per bit, byte or packet? What about which protocols are being most heavily utilized on a particular subnet?

### Security

- Easily configure DNS caching time limits
- See all traffic 'Host to Host' or 'Subnet to Subnet'
- Easily filter and display traffic based upon TCP flags
- Track flow sequence numbers to trend traffic patterns
- Quickly identify MITM servers on the network (DNS, DHCP, SMB, etc.)

With all of these great features it's no wonder Scrutinizer is invaluable when it comes to security. Administrators can toggle between various reports to easily identify traffic flowing from host to host or subnet to subnet. Tracking flow sequence numbers and trending traffic patterns has never been easier. Further, Scrutinizer can quickly identify rogue servers placed on the network attempting a Man-in-the-Middle attack against such services as DNS, DHCP, SMB, and more.

### Supported Protocols & Other Technical Specifications

- Granularly define reports down to specific interfaces across multiple routers, switches, or firewalls
- Easily integrate 3rd party application and URLs into dashboards
- Integrates with LDAP servers
- Support for SNMPv1, SNMPv2c, and SNMPv3
- Support for all industry standard flow analytics (IPFIX, NetFlow v5, NetFlow v9, FnF, sFlow, J-Flow)
- Configurable to over 1000 interfaces and several hundred exporters
- Create filters based upon next routing hop
- Filter on any exported field such as VLAN id, L2 Address, L3 Address, and latency
- Immediate cost savings by not requiring the purchase of an expensive Microsoft Database server
- Capable of handling up to 20,000 (40,000 with the Virtual Appliance) flows per second on an unlimited number of UDP ports

From a technological stand-point Scrutinizer leaves similar priced flow analyzer products in the dust. Scrutinizer's robust and superior features such as LDAP integration and support for every industry standard flow protocol in the market today provide enormous value. When configured appropriately the Scrutinizer engine can receive up to 20,000 (40,000 with the Virtual Appliance) flows per second on over 1,000 different interfaces. Customizable dashboard 'mashups' allow for 3rd party applications and URLs to be imported directly into Scrutinizer making it the only application needed to know exactly what's on the network.

### Troubleshooting

- Easily identify link failures
- Easily identify specific link traffic statistics
- Easily identify QoS across the network by analyzing jitter & latency
- Easily find out where the 'slowness' on the network is occurring
- Plan for network growth

Administrators can use Scrutinizer to monitor the volume of traffic on their network and analyze how it fluctuates over time. In fact, Scrutinizer's 'network volume gadget' feature can be utilized to see the number of unique hosts and well known applications being accessed. This report shows trending information on the number of hosts accessing the network providing the IT administrator with insight into increases over time. Additionally, reports can be limited by time range (such as 9am to 5pm) to monitor network traffic volume during peak business hours.

Scrutinizer can also be used to identify bottlenecks on the network. For example, when streaming video or VoIP is deployed on the network, automatic alerts could be configured in Scrutinizer to email the IT administrator notifying him of packet-loss, delays in packets arrival, or packets arriving out of order. This provides an IT admin the ability to proactively know of call quality degradation even before users complain of an issue.

### Visibility

- Trend analysis reports on archived data
- Easily see the top 5 interface across all routers, switches & firewalls
- Integrated Google Maps viewing allows for visual representations of distributed network
- Flexible viewing options allow data to be seen from different angles (pie, bar, matrix, line)

Various viewing options within Scrutinizer, such as the matrix view provide an innovative tool for better visualization of traffic flows. Based on criteria established when the report is generated, administrators can toggle to different views to see a graphical map of where traffic is flowing. The 'Matrix' enables administrators to easily visualize which systems a particular host has been accessing.

## *Flow Analytics Module*

The Flow Analytics Module brings traffic flow diagnostics to the next level by adding historical reporting for an unrestricted period of time, advanced alarming with the ability to set thresholds, role-based administration, and in-depth traffic analysis algorithms to the Scrutinizer software. It can easily identify top applications, conversations, flows, protocols, domains, countries, and subnets on the network, as well as watch for and alert on suspicious or potentially hazardous network behavior patterns thereby providing administrators with greater network security awareness.

In addition to the base-level features Scrutinizer with the add-on Flow Analytics module provides several additional advanced features, such as:

- Flexible Reporting
  - Dell SonicWALL specific templates for reporting
  - Special traffic analysis reports such as Flow Volume & NBAR Support
  - MPLS reporting by subnet
  - Microsoft Exchange log trend analysis
  - Puts information at administrators fingertips
    - Easily identify the top applications being utilized on the network
    - Easily identify the top country of origin for traffic flowing across the network
    - Easily identify the top domains being accessed
    - Easily identify the top subnets being utilized on the network

With the addition of the Flow Analytics module Scrutinizer becomes an even more powerful reporting engine offering even greater flexibility and granularity. In addition to all the reporting functions provided in the base edition, Scrutinizer with Flow Analytics adds advanced reporting options such as flow volume, MPLS by subnet, Microsoft Exchange log trending and NBAR support. Administrators have with a wealth of information right at their fingertips.

IT administrators can create custom reports by applying filters to granularly define the specific information desired. Once created, custom reports can be saved for later use. Custom Reports allow the user to configure detailed reports by filtering on fields such as: IP Addresses, ranges and subnets; Port numbers and ranges; Defined applications including ranges of protocols and groups of protocols; Multiple interfaces from different routers and switches; Any exported field available via NetFlow or IPFIX; Dynamic QoS monitoring; Detailed security / forensic information.

The Flow Analytics Module adds several additional flow based traffic analysis report types. Examples include but are not limited to: Granular IPFIX based application visualization reports for Dell SonicWALL products; Flexible NetFlow NBAR based application reports (requires IOS v15 on Cisco routers); Conversations to/from host pairs and applications used; Flow reports with ToS field; Host flow reports to show hosts sending or receiving the most flows; Host volume reports to show the volume of unique hosts per second; Pair volume reports to show the volume of unique to/from address pairs per second.

- ‘Set It & Forget It’ Alerting
  - Easily create alerts to notify administrators of unfinished flows or nefarious activities
  - Alerts can trigger email notifications, SNMP traps, syslog messages, and script execution (facilitating event remediation)
  - Alarms can be configured to alert administrators based upon specific interface utilization
  - Administrators can be alerted based on any pre-defined report
  - Reports can be scheduled, then emailed to administrators
  - Administrators can proactively monitor QoS of RTSP traffic

The Flow Analytics add-on to Scrutinizer provides administrators with greater automation control making routine advanced reporting a snap. Alerts can be configured based upon everything from unfinished flows to specific interface utilization. Further, administrators can configure QoS thresholds to proactively be alerted of RTSP latency and jitter before end users even reports a problem.

Using saved Scrutinizer reports, the Flow Analytics Module can monitor and send out syslogs when traffic patterns violate specified thresholds. For example, the Flow Analytics Module can be used to monitor an application for a certain ToS within a class A subnet.

The enhanced security functionality alone makes Scrutinizer with Flow Analytics an invaluable tool in an administrator’s arsenal. Know exactly what is happening on the network- where traffic originated, where it is going and what type of traffic it is. Is someone planning an attack by scanning the corporate network? Did one of the servers get infected with malware and launch a DDoS attack? Scrutinizer can automatically detect these activities and alert administrators immediately upon detection.

At the heart of Scrutinizer’s attack detection capabilities are a behavioral analysis engine and a periodically updated known threats database. IT administrators can use Scrutinizer to identify and alert on threats such as DDoS attacks, port scanning, attacks from infected hosts behind the firewall. In turn this allows the administrator to remediate threats by making configuration changes, by disabling ports, and modifying ACLs, on routers, switches and firewalls. Scrutinizer uses configurable algorithms to analyze flow data from the entire network infrastructure, or from a pre-configured sub-selection of devices and exporter tables to automatically send syslog messages when trouble arises. Using Scrutinizer IT staff can identify: RST/ACK worms, zero-day worms, SYN Floods, DoS, DDoS attacks, NULL, FIN, XMAS scans, port scanning, P2P file sharing, Excessive ICMP unreachable, Excessive Multicast traffic, Prohibited traffic being tunneled through allowed protocols (DPI on TCP port 80), Known compromised internet hosts, illegal IP addresses, Policy violations and internal misuse, Poorly configured or rogue devices, Unauthorized application deployments

The Flow Analytics Module can utilize the local DNS to resolve IP addresses in real-time. This allows Scrutinizer to group traffic into domains without having to define ranges of IP addresses which could otherwise quickly become a nightmare to manage. With this feature, Scrutinizer can be configured to monitor traffic to or from specific domains and alert an administrator when preconfigured thresholds are met or exceeded.

The history of repeat offenders can be easily identified through the use of a Unique Index (UI) to manage traffic counts. In addition, the Flow Analytics Module helps locate machines involved with DDoS attacks or infected with viruses/worms.

The Flow Expert Window provides insight to immediate network problems as they occur to identify and resolve DoS attacks, bottlenecks, network scans, improperly terminated connections and more. Traditionally, the functionality provided by this "Expert Window" feature has only found in packet analyzers.

- Supported protocols & other technical specifications
  - Support for L7 application awareness by using NBAR or IPFIX
  - Automatic DNS resolution

### Advanced Troubleshooting

The Flow Analytics Module enables advanced troubleshooting techniques, such as:

- Begin capacity planning for growing networks
- Easily identify the volume of flows per host
- Easily identify the volume of traffic flowing between a pair of hosts
- Easily identify the volume of unique hosts per second traversing the network
- Peer into VoIP traffic when using IPFIX to see granular metrics such as codec & caller ID

Tired of looking at a list of meaningless IP addresses? Wouldn't it be great if the flow-analyzer could perform reverse DNS lookups on those addresses in real time? Want to know what specific Web 2.0 applications are being accessed on the network? Scrutinizer with the Flow Analytics module can do all that. Administrators running Flexible NetFlow with NBAR or IPFIX with extensions can easily identify applications such as YouTube, Facebook, eBay and more instead of just seeing 'TCP port 80' on the report.

IT administrators can use Scrutinizer to analyze Voice over IP (VoIP) traffic and determine: the amount of voice traffic into and out of the network over time; what users are involved with the most VoIP traffic; the caller ID of destination and source; QoS statistics such as Latency/Jitter and packet loss of each call; what audio codec is being utilized; and whether the router is modifying DSCP values.

By using multiple servers to act as distributed flow data collectors, Scrutinizer can be deployed as a distributed solution accessible through a single central web based interface allowing for easy scalability to support enterprise level networks.

Dozens of distributed collectors can be deployed and, depending on the volume of flow data being received by each collector, a single deployment of Scrutinizer can potentially support hundreds of firewalls, routers and switches.

Network topology maps come to life in Scrutinizer as links change in color and thickness with variations in network utilization. Clicking on a link in a network topology map brings up useful traffic statistics such as top talkers and top conversations within the last minute.

IT administrators can use Scrutinizer to plot network appliances such as firewalls, routers, and switches on a Google map embedded in the Scrutinizer application. Using this geographic map as a starting point into all network analysis provides traffic details collected and organized for easy visualization in Scrutinizer.

## *Multi-Tenancy Module*

The Dell SonicWALL Multi-Tenancy Module (only available as an add-on for Dell SonicWALL Scrutinizer with the Flow Analytics Module,) adds several features that are especially useful for Managed Service Providers (MSPs) and Internet Service Providers (ISPs).

As a service provider or IT organization, delivering information about the performance of the infrastructure and services you are providing to the end-user is critical. With Scrutinizer MTM, you have the secure flexibility needed to deliver a controlled, secure and segregated reporting experience per customer or user.

- Allows permissions to be configured per router / switch / interface, etc. per login account.
- Style Sheets are easily modified with several defaults to change the colors and fonts to match the Service Providers marketing efforts. Most logos can be changed as well.
- Definable default landing page when customer logs in.
- Unique language support per login account.
- Allows integration of 3rd party applications and URLs into mashups.

### Mashups for easy accessibility

Utilizing simple web technology, Scrutinizer allows anyone to easily assemble a URL into a mashup or third party application to directly import and display important information regarding the activity of a specific host or application on your network into the Scrutinizer dashboard.

### Customer portal

IT administrators can choose to provide end users with secure login access to the flow data generated by their network devices. End users can also use the customer portal to troubleshoot bandwidth usage and identify/analyze odd traffic patterns. Additionally, automatic HTML reports can be scheduled for each end customer. Service providers can use the portal as a message board to communicate with their customers as well as integrate other applications into the Dashboard interface.

## *Advanced Reporting Module*

The Dell SonicWALL Scrutinizer Advanced Reporting Module is a value added performance monitoring, reporting, and billing solution. It provides extended performance monitoring and reporting for Cisco and Citrix solutions. It also offers CrossCheck, which provides integration with third party monitoring tools such as WhatsUp Gold, Orion, SNMPc, Uptime Devices, Nimsoft and others. In addition, it allows customizable billing and invoicing based on actual network usage.

### Report Designer

The Report Designer allows users to create their own report templates based on the flow templates they are receiving.

### Extended Support for Cisco Solutions

The Scrutinizer Advanced Reporting Module supports Cisco Smart Logging and Telemetry, Cisco TrustSec (CTS), Cisco Performance Routing (PfR), Performance Agent and Performance Monitoring (Cisco Medianet). This module delivers detailed reports on all traffic related to voice and video. IT staff can easily use this module to troubleshoot issues related to video or voice by using Scrutinizer to analyze the appropriate flows.

With the Scrutinizer Advanced Reporting Module, Scrutinizer can be configured to analyze and alert on excessive amounts of one or a combination of the following example parameters:

Round Trip Time (Latency)

- Jitter
- Packet Loss
- Bits, Bytes and Packets
- MAC Addresses, IP Addresses
- VLANs
- Domains
- Applications
- Interface
- Hundreds more not listed

### Extended Support for Citrix Solutions

The Scrutinizer Advanced Reporting Module brings enhanced support for Citrix equipment by adding granular drill-down capabilities for:

- URLs providing reporting insight into web servers and databases being accessed
- Applications providing reporting insight into applications being accelerated via NetScaler
- Latency providing reporting insight into the health and delay as seen by NetScaler

**Note**: Citrix NetScaler makes applications and cloud-based services run five times better by offloading application and database servers, accelerating application and service performance, and integrating security.

### CrossCheck

The Scrutinizer Advanced Reporting Module also includes CrossCheck which was created in direct response to large MSP and enterprise customer demands for integration with third party monitoring applications. It provides:

- An inventory of all network devices managed by other analytic tools displaying several attributes including device name, IP address, and status.
- Flowalyzer Poller, which continually assesses the status of devices identified by Advanced Reporting and provides updates to Scrutinizer via IPFIX messages.
- References on the status of devices inside third party management solutions, and a single Fault Index value across multiple integrations. Fault index measurements indicate device status across numerous management systems using configurable severity levels. Syslog notifications can be sent out if predefined threshold levels are met.
- Clickable inventory item listings that provide users with direct links to integrated third party applications and easy access to devices that are managed via these other applications.
- The ability to create inventory groupings for easy monitoring of network segments regardless of whether the appliances are managed by Scrutinizer or a third party application.

### Customizable Traffic and Usage-based Billing and Invoicing

The Scrutinizer Advanced Reporting Module enables customizable invoicing and billing solutions based on actual network usage, and eases data export to Microsoft Excel in .CSV format.

The Advanced Reporting Module allows service providers to export flow data based on any flow (NetFlow, IPFIX, sFlow, etc.) field or combination of flow fields including but, not limited to: rate per second, packets, total bits, IP addresses, ToS (DSCP) or BGP autonomous system (AS) number. This data can then be used to invoice end customers based on actual network usage rather than WAN connection speed.

The Advanced Reporting Module routinely exports a custom .CSV file with all the required details. For example, it allows billing based on a flat rate versus a burst rate as well as total amount transferred per month. More traditional billing is also possible, for example, where the end customer pays based on the 95% percentile technique.

## *Flowalyzer NetFlow & sFlow Tester*

Separate from Scrutinizer and its add-on modules, Dell SonicWALL also offers a free tool called Flowalyzer NetFlow & sFlow Tester.

Flowalyzer is a free NetFlow and sFlow Tool Kit for testing and configuring hardware or software to send and receive NetFlow / sFlow data.

Flowalyzer can help IT professionals troubleshoot hardware from vendors like Cisco and Enterasys, as well as NetFlow collector software, ensuring that whichever flow technology they use is configured properly on both ends.

### Flowalyzer NetFlow & sFlow Listener

- Determine which flow sending devices are sending the highest volume
- Listen for NetFlow on multiple ports
- Display packet count, version of NetFlow and UDP port flows are coming in on
- Display the IP address and DNS name

### Flowalyzer NetFlow Generator

- Generate NetFlow data to determine if the destination collector is accepting flows
- Send NetFlow v5, NetFlow v9, and IPFIX
- Determine if the destination collector is dropping NetFlow data by comparing the flows sent to what is received on the other end

### Flowalyzer NetFlow & sFlow Configurator

- Configure Cisco Routers or Enterasys switches for exporting NetFlow data
- Uses SNMP to make OID sets
- Supports SNMP v1, v2c, and v3

### Flowalyzer NetFlow & sFlow Communicator

- Run a ping or trace route to any host
- Ping via ICMP, UDP or TCP protocols
- Communication responses are readable in a clear response display

### Flowalyzer SNMP Trender

- Generate trend graphs for any SNMP-enabled device
- Custom OID support allows any SNMP variable to be trended in real-time
- Custom update period allows graphs to update as often as every second
- Supports SNMP v1, v2c and v3
- Save multiple sets of Read/Write SNMP credentials
- No limit to the number of simultaneous graphs

## System Requirements

Dell SonicWALL Scrutinizer 11.5.2 is supported on systems with the following:

### Windows Appliance

| Component | Minimum Specifications (for trial installations) | Recommended Specifications (for production environments) |
|---|---|---|
| RAM | 4 GB | 8 GB |
| Disks | 50 GB IDE or SATA | 1 TB or more, 15K SCSI in a RAID 0 or 10 configuration |
| Processor | 2 Core, 2 GHz or more | 4 Core, 2 GHz or more |
| Operating System | Windows 7 or 8<br>Windows 2008 or 2012 | Windows 2008 or 2012 Server |

### Virtual Appliance

| Component | Minimum Specifications (for trial installations) | Recommended Specifications (for production environments) |
|---|---|---|
| RAM | 16 GB | 64 GB or more |
| Disks | 100 GB | 1 TB or more, 15K RAID or 10 configuration |
| Processor | 1 CPU, 4 Cores, 2 GHz or more | 2 CPUs, 8 Cores, 2 GHz or more |
| Operating System | ESX4, ESXi4, ESX5, ESXi5 | ESX4, ESX5 |

### Note

- On a Dell SonicWALL network security appliance, the Scrutinizer NetFlow/IPFIX implementation in SonicOS 5.8 and higher is available when the Dell SonicWALL™ Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, and Application Intelligence and Control Service, for the Application Intelligence and Control service or for the Comprehensive Gateway Security Service suite (CGSS). NetFlow/IPFIX is supported on the Dell SonicWALL TZ 210 series, TZ 215 series, and all NSA series appliances. See the latest *SonicOS Release Notes* for more information about SonicOS features that require additional licensing.
- Smartphone and Tablets running iOS 6 and higher or Android 4.2 and higher are supported.

## New Features in Scrutinizer 11.5.2

This section lists the new features in the Dell SonicWALL Scrutinizer 11.5.2 release.

- **AVC Reporting** – Voice and video identification to AVC reporting has been added.
- **VRF ID Enhancements** – Improvements have been made to VRF ID descrptions.
- **"Chassis" Report Enhancements** – Two new IANA "Chassis" Report types have been added.
- **NAT Enhancements** – New NAT source and destination details reports have been added.
- **IPFIX Report Enhancements** – New IANA Open vSwitch IPFIX reports have been created.
- **Cisco PfR Support** – A Cisco Performance Routing (PfR) Root Cause Delay report has been added.
- **Cisco VoIP Report Enhancements** – CBQoS and RTP Payload have been added to the Cisco VoIP Report.
- **Language Translations** – New Chinese and Japanese translations are available.

## Resolved Issues

The following issues were resolved in the Scrutinizer 11.5.2 release:

| Issue # | Description |
|---|---|
| 13592 | OpenSSL HeartBleed Vulnerability. A flaw in OpenSSL allows attackers to capture sensitive information. |
| 11760 | The Flow Hopper indicates a yellow icon, although there is no obvious problem. |
| 12782 | The Report Map link does not display measurements or report names. |
| 12907 | The Subnet Filter vs IP Group report results do not match for the same subnets. |
| 13070 | Improvements were made to the method that adds devices that adds devices to the Threat Index Threshold Algorithm. |
| 13076 | There are no results when the Alarms tab is clicked. |
| 13118 | Interfaces that do not have speed information do not render correctly in maps. |
| 13156 | The Alt Tag for "NONE_AVAILABLE" in the Username by IP reports is unclear. |
| 13158 | Improvements were made to the Alarms gadget filter storage. |
| 13176 | Maps with special characters in the label names do not save. |
| 13186 | The Device Explorer has a device three recursion error (Groups within Groups). |
| 13190 | Some saved reports are not modified properly during an upgrade. |
| 13193 | Improvements were made to the Host Flows report table. |
| 13197 | The Top Applications gadget intermittently displays no data after a refresh. |
| 13201 | The Alarms tab gets stuck after using "Copy Existing Policy." |

| | |
|---|---|
| 13203 | Map Links are not converting bits correctly. |
| 13204 | User is unable to delete orphans when using a filter. |
| 13207 | If plixer.ini exists, no error message displays when an install fails. |
| 13209 | The summary NBAR table does not populate from Cisco WLC. |
| 13219 | “Check for Updates (NULL)” is in the System Menu. |
| 13221 | Changing time granularity in business hours generates an error. |
| 13236 | Scrutinizer has problems on Chinese and Japanese Windows servers. |
| 13237 | Interface descriptions from the option templates are not working. |
| 13242 | High-speed logging host to host has event reporting issues. |
| 13249 | Extreme exports have “Probe Reports.” Menu-Move these reports to Pairs. |
| 13298 | Inbound Threshold Filter causes incorrect alarms when added with the ‘less than’ sign (<). |
| 13300 | Changes to the admin password in the UI do not sync successfully. |
| 13308 | Notification profile processing of the source (%s) parameter is more user-friendly. |
| 13314 | The Report Designer > Select Temple dropdown displays the old template. |
| 13315 | The NetScalar report Alt Tag has decoding/formatting issues. |
| 13324 | The FA vertical text does not use valid Chinese characters. |
| 13330 | The Emailed IP Groups report includes a line item for “NO_VALUE.” |
| 13332 | An increase of email occurs on demand timeout. |
| 13334 | The status of icons does not properly reflect the fault index. |
| 13340 | Changing the default unit to another unit in the Top Interfaces dashboard gadget causes the gadget to hang and not respond. |
| 13363 | NBAR category changes are allowed. |
| 13364 | Excluding IPs from the Nefarious Activity Algorithm does not successfully exclude IP addresses. |
| 13380 | Top applications and subnets do not populate. |
| 13411 | The “Click to see all…” text is not always correct (Alarms). |
| 13422 | The table colors are incorrect when report order by columns is clicked. |
| 13452 | The alarm notification on the first violation only is not working. |
| 13464 | Changes to the admin password results in being booted back to the Login screen upon next log in. |

| | |
|---|---|
| 13469 | The languages.chinese_zh_TW is not correct on Linux systems. |
| 13475 | The installer should open firewall ports on Windows 2012. |
| 13653 | Fixes are needed for the NetFlow v8 decode error for port protocol aggregation. |

## How to Upgrade to the Licensed Version

Click the Scrutinizer link on the www.mySonicWALL.com homepage to automatically register a Scrutinizer product with its own serial number. The user is then directed to the Services Management page for the newly registered Scrutinizer product. Upon registration, Dell SonicWALL Scrutinizer will be available from the Downloads section in mySonicWALL.

The free trial version of Scrutinizer can be installed immediately and does not require a license key; just double click the executable and follow the installation process.

The new Scrutinizer product will be listed in the My Products section on mySonicWALL. Click on the Scrutinizer product to bring up the Services Management page for that particular product.

Additional software modules and support licenses can be activated on the Services Management page either by clicking on the Buy Now button or by either entering the appropriate keys purchased from a Dell SonicWALL reseller or distributor.

Upon activation of any additional licenses, an email with instructions on how to download a license file will be sent to the email address associated with the mySonicWALL account. The license file will be available in the My Downloads section of the Download Center of MySonicWALL.

Once a license file is obtained, bring up the Dell SonicWALL Scrutinizer web interface, i.e. the Scrutinizer application itself, and click on the Admin tab. In the left navigation bar, click **Settings > Licensing**. Paste the license key into the appropriate box. Click the **Save** button.

### *Installed Based Upgrade Considerations*

In the licensing model for add-on modules, the following applies:

- The Cisco Advanced Reporting Module, Citrix Advanced Reporting Module, Cross Check Module and the billing component of the Service Module have been combined in the Advanced Reporting Module
- Multi-tenancy features of the old Service Provider Module are now separate in the Multi-Tenancy Module

When upgrading, the following rules will be employed in the license mapping:

- Deployments licensed for the Flow Analytics Module at the unrestricted node level which are upgraded to 11.5 will be licensed for the Flow Analytics Module at the 250 node level
- After upgrading to 11.5, any deployment licensed for one or more of the following modules will be licensed for the Advanced Reporting Module at the exporter node count equal to their current 11.5 Flow Analytics license
  - SonicWALL Scrutinizer Managed Service Provider Module software license
  - SonicWALL Scrutinizer Cisco Advanced Reporting Module software license
  - SonicWALL Scrutinizer Citrix Advanced Reporting Module software license
  - SonicWALL Scrutinizer Cross Check Module software license
- After upgrading to 11.5, any deployment licensed for the service provider module will be licensed for the Multi-Tenancy Module at the exporter node count equal to the current 11.5 Flow Analytics license
- Virtual appliance will have a free version available for download but for the 30 day trial the customer will need a separate application license generated by Plixer

## FAQ

- **What is NetFlow?**

  Cisco® NetFlow technology is an embedded feature within Cisco IOS routers and high end switches (e.g. 6500 series). NetFlow data records consist of information about source and destination addresses, along with the protocols and ports used in the end-to-end conversation. Scrutinizer uses this information to generate graphs and reports on traffic patterns and bandwidth utilization. More information can be found here.

- **What is sFlow?**

  Unlike NetFlow which aggregates multiple conversation streams into a single packet, sFlow is a packet sample of traffic. Although it offers 100% of the packet, when used strictly for IP accounting, it is unreliable.

- **What are the different versions of NetFlow available?**

  Version 1 is the original format supported in the initial NetFlow releases, while version 5 is the standard and most common NetFlow version deployed. Version 5 is an enhancement that adds Border Gateway Protocol (BGP) autonomous system information and flow sequence numbers. Version 6 is similar to version 7. This version is not used in the new IOS releases. Version 7 is an enhancement that exclusively supports NetFlow with Cisco Catalyst 5000, 6500 and 7600 series switches. Version 8 is an enhancement that adds router-based aggregation schemes. It was introduced to reduce resource usage, and includes a choice of eleven aggregation schemes. Version 9 is an enhancement to support different technologies such as Multicast, Internet Protocol Security (IPsec), and Multi-Protocol Label Switching (MPLS). Versions 2, 3 and 4 either were not released.

  Scrutinizer currently supports:

  - NetFlow versions 1,5,6,7 and 9
  - sFlow version 2, 4 and 5
  - Flexible NetFlow, IPFIX, JFlow and NetStream

- **How is NetFlow different from traffic analyzers like MRTG?**

  MRTG and other such equivalent tools provide information that is largely limited to SNMP statistics. NetFlow is more geared toward application-level details such as hosts, protocols, and conversations, which are an inherent part of IP traffic.

- **Is Cisco the only vendor supporting NetFlow?**

  NetFlow technology was invented by Cisco, and Cisco IOS devices offer NetFlow compatibility. There may be other vendors offering NetFlow support on their devices. Scrutinizer has been tested on over a dozen different vendors.

- **Is a trial version of Scrutinizer available for evaluation?**

  Yes. A free version of Scrutinizer can be downloaded and you can get an evaluation license to try the full version.

- **What are the differences between the free and commercial version?**

  The commercial version of Scrutinizer NetFlow & sFlow Analyzer includes the Flow Analytics add-on module, which adds historical data retention and network behavior analysis.

- **What are the system requirements?**

  Scrutinizer's system requirements are detailed here: System Requirements

- **How do I find out if my Cisco equipment supports NetFlow?**

  Review the NetFlow Services Solutions Guide to find out if you have a NetFlow compatible Cisco router or switch.

- **What if I need features that Scrutinizer does not support?**

  We understand that our software needs to be flexible. If you want a feature added, we may be able to work with you.

- **Does it support other Languages?**

  Scrutinizer currently supports the following languages; Chinese (Simplified and Traditional), English, French, German, Japanese, Korean, Portuguese, Russian, and Spanish.

- **How will enabling NetFlow affect the performance of the router/switch?**

  For detailed information on exactly how enabling NetFlow will affect the performance of your Cisco router or switch, review the NetFlow Performance Analysis whitepaper [PDF]: http://www.cisco.com/en/US/technologies/tk543/tk812/technologies_white_paper0900aecd802a0eb9.html.

- **How long do I have to wait before the graphs are populated?**

  Less than 5 minutes. Make sure you have the NetFlow configured correctly on the router or switch.

- **Why are some interfaces labeled as IfIndex2, IfIndex3 or just 1, 2, 3, etc.?**

  This happens if the interfaces did not respond to the SNMP requests sent by Scrutinizer. Bring up the SNMP view that lists all the interfaces and click the Update button. Please review SNMP Device View in the Scrutinizer manual.

  Also, this will occur if flow option templates to identify the interfaces have not been received.

- **How do I enter IP to name resolutions so that Scrutinizer doesn't have to use the DNS to resolve IPs?**

  Edit this file: C:\WINDOWS\system32\drivers\etc\hosts and enter the IP to name translations.

- **Overall utilization on the interface appears to be understated. Why would this be?**

  1. Make sure NetFlow is enabled on all physical interfaces of the device. Do not be concerned with the virtual interfaces, as they will auto-appear once NetFlow is enabled on the physical interface.
  2. If the hardware can't keep up with sending the NetFlow packets, it will drop NetFlows before they even leave the device. To check to see if this is the problem, login to the Cisco device.
     Command to type: Router_name>**sh ip flow export**

     At the bottom of the export, look for something like "294503 export packets were dropped due to IPC rate limiting". If this counter is incrementing, the hardware cannot keep up with the export demands.
  3. The command below breaks up long-lived flows into 1-minute segments. You can choose any number of minutes between 1 and 60; if you leave the default of 30 minutes you will get spikes in your utilization reports. Command to type**: ip flow-cache timeout active 1**
  4. The command below ensures that flows that have finished are exported in a timely manner. The default is 15 seconds; you can choose any value between 10 and 600. Note however that if you choose a value that is longer than 250 seconds Scrutinizer may report traffic levels that appear low.
     Command to type: **ip flow-cache timeout inactive 15**

     NetFlow only exports IP traffic (i.e. no IPX, etc.) and no layer 2 broadcasts are exported by this version of NetFlow.

- **How do I setup my router to forward NetFlows to two destinations?**

  Type the "ip flow-export destination" command twice:

  - router-name# **ip flow-export destination 10.1.1.8 2055**
  - router-name# **ip flow-export destination 10.1.1.9 2055**

- **Why are my graphs reporting over 100% utilization?**

  1. The interface speed is not correct. Scrutinizer uses the speed specified in the SNMP OID. Login to the router or switch and fix the problem or in Scrutinizer go to Device Details and manually type in the correct speed.
  2. The active timeout has not been set to 1 minute on the router. Login to the router or switch and fix the problem.
  3. Non-dedicated burstable bandwidth, where the ISP allows you to use over the allocated bandwidth.
  4. Both ingress and egress NetFlow collection have been enabled on the interface. This can work properly if the direction bit is set in the egress flows. Scrutinizer works ideal when only ingress NetFlow collection is configured on all interfaces. Only egress on all interfaces is also possible.
  5. Do you have any encrypted tunnels on the interface?
     - 47 - GRE, General Routing Encapsulation.
     - 50 - ESP, Encapsulating Security Payload.
     - 94 - IP-within-IP Encapsulation Protocol.
     - 97 - EtherIP.
     - 98 - Encapsulation Header.
     - 99 - Any private encryption scheme.

     This can cause traffic to be counted twice on an interface. In Scrutinizer, go to Admin Tab > Definitions > Manage Exporters. Click on the round icon with the '-'. When you mouse over the icon, the ALT will display "View the current protocol exclusions of this device." Click on this and make sure the above protocols are being excluded.
  6. Full Flow Cache: All flows are stored in the flow cache on the router before export. Once the cache is full, it stops adding entries into the cache until it expires them. When events such as a DDOS or a "social event" occur, the router's cache becomes full. The cache can be increased; however, it will use more memory and could have a negative impact on the router. A loss of flows will cause Scrutinizer to understate utilization.

- **How do I find out if any updates are available for Scrutinizer?**

  In your local Scrutinizer install, click the Status tab. If updates are available, you will see a spinning blue icon in the upper right hand corner. If you have a proxy server, this spinning icon will always appear. Click on it to find out the latest version.

  Users can also use the **-v** parameter for any **\scrutinizer\cgi-bin*.cgi** or **\scrutinizer\bin*.exe** file to get the current version and build for that executable.

  Example: **scrut_util -v**

  Compare this to the Scrutinizer Update History.

- **I have forgotten my Scrutinizer password. How do I find out what it is?**

  In your local Scrutinizer install, type the following commands in a command prompt, from the [homedir]\bin\ directory:

  **scrut_util.exe -reset_admin_password** [USERNAME]

  The USERNAME is the name of the Scrutinizer user account to modify. When the command is executed, it will prompt for the new password, and then to re-enter it.

  **Note**: These commands must be run from the Scrutinizer server.

- **How do I setup SSL with Scrutinizer?**

  An installer with SSL support is available for eligible parties. Please contact us for the SSL installer.

- **How do I use a different drive for storing data?**

  **Note**: The following procedures will not work for remote drives based on Windows shares.

  1. Stop the plixer_mysql service.
  2. Copy the **[homedir]\Scrutinizer\mysql\data** directory to the new drive.
  3. Edit the **[homedir]\Scrutinizer\mysql\my.ini** file, changing the drive letter for the **datadir=x:[homedir]/SCRUTINIZER/mysql/data/** entry.
  4. Start the **plixer_mysql** service.

  For more information on using a different drive for stored data or storing data to a remote database with Scrutinizer version 7 or higher, review this guide.

- **Why do not all of the colors print correctly when I try to print an emailed report?**

  This can be caused by an option found in some browsers and email clients.

  In Internet Explorer:

  1. Open the "Tools" menu.
  2. Click "Internet Options.
  3. Click the "Advanced" tab.
  4. Scroll down to the "Printing" section.
  5. Check "Print background colors and images.
  6. Click "OK."

  This change will carry over to Outlook and Outlook Express.

- **Can Scrutinizer run in VMware?**

  Yes, please contact support for more information on the Scrutinizer Virtual Appliance.

- **How do I exclude Scrutinizer in Symantec Antivirus?**

  1. From within Symantec, expand the "Configure" option from the tree menu and select "File System."
  2. Click the "Exclusions" button.
  3. Click the "Files/Folders" button.
  4. Find the Scrutinizer directory and check the box next to it.
  5. Click "OK" to finish.

- **Why are my IPs not resolving, even though I have configured my DNS properly in Windows?**

  In certain situations, Scrutinizer may not be able to properly resolve IP addresses. This usually happens when there are multiple DNS servers with disparate records. To deal with this, Scrutinizer allows you to specify your DNS servers in a file rather than get the settings from the Windows Registry. The steps are outlined below:

  1. Create a file in the **\scrutinizer\html** directory called **dns.conf**.
  2. Open this file with a text editor like Notepad.
  3. Create a list of DNS servers in the file in the format below.
     - nameserver 192.168.1.1
     - nameserver 166.186.184.2
     - nameserver 224.39.1.171

  Now that you have created this file, you should now be able to go into the Scrutinizer web interface and do lookups properly.

- **I'd like to change the MySQL "scrutinizer" user password from the default to something more secure. Is there anything else I need to do other than set the password in MySQL?**

  Update MySQL Root password via CLI using **scrut_util.exe** located in the **[HOMEDIR]\Scrutinizer\bin** directory. There is a two-step process, resetting the password then updating the **plixer.ini** file.

  Options:

  -**reset_mysql_password**

  Changes the MySQL root account password:

  -**update_plixerini_mysqlroot**

  Use this command to update the **plixer.ini** database root user password. Scrutinizer and the database root password must be in sync.

  Usage Example:

  **C:\Program Files (x86)\Scrutinizer\bin>scrut_util.exe -reset_mysql_password**

  Changing Password for MySQL Root Password: Press <ENTER> to abort.

  **Note**: On Windows 2008/2012 and Windows 7, you must run this command from the Administrator Command Prompt

  New Password:

  Verify Password:

  Attempting to login with new password ... PASS!

  Password Updated for MySQL Root ... DONE!

- **Where can I find the Scrutinizer manual?**

  A copy of the Scrutinizer manual is included with your product. Just click any of the "?" icons.

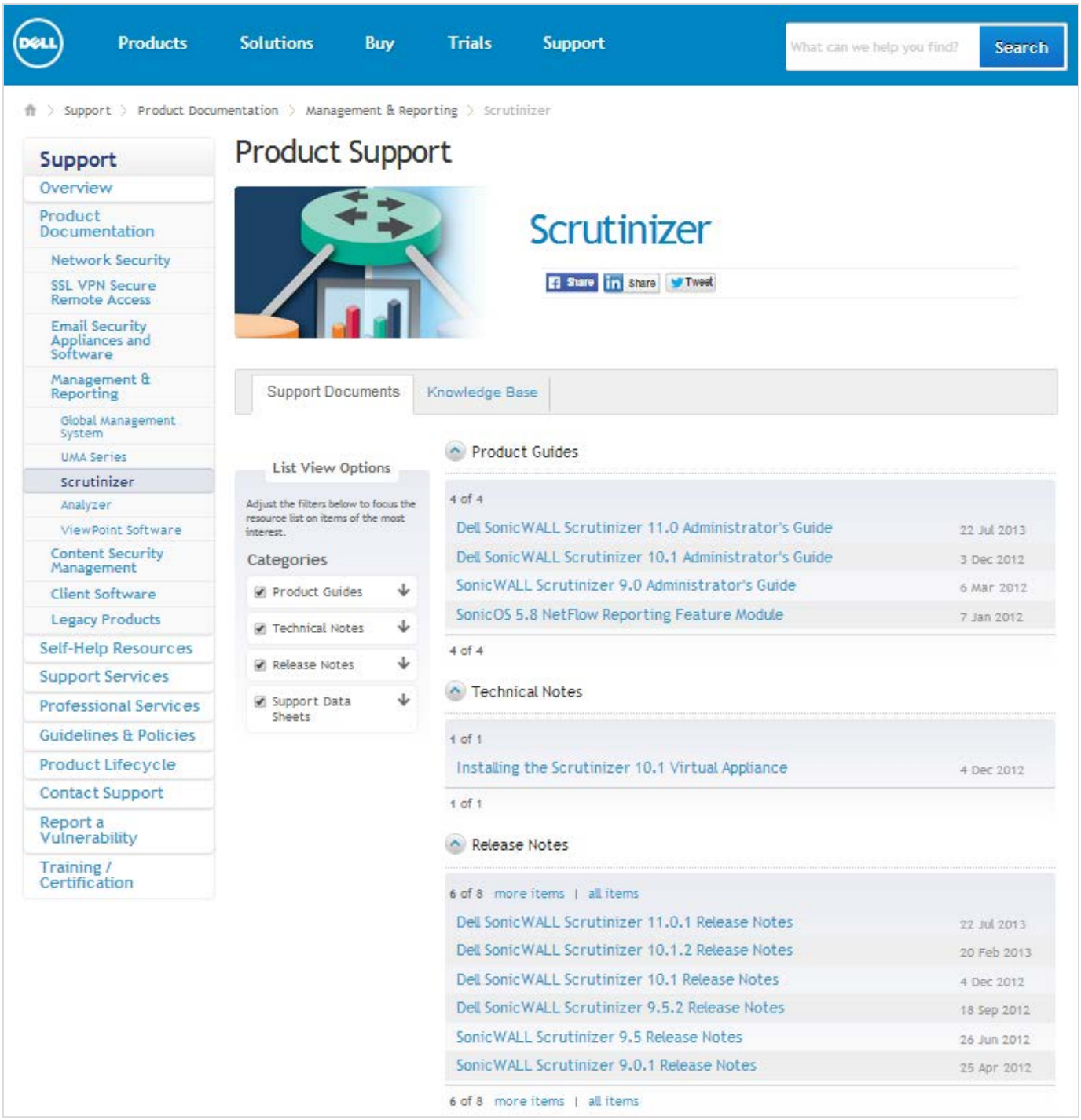
- **How do I know how much hard drive space I will need?**

  Use the NetFlow Bandwidth and Hard Drive Consumption Calculator to determine how much hard drive space your NetFlow data will consume.

## Related Technical Documentation

Dell SonicWALL Scrutinizer reference documentation is available at the Dell SonicWALL Technical Documentation Online Library: http://www.SonicWALL.com/us/support/6632.html

More information on NetFlow Services is available on the Dell SonicWALL Web site.




Last updated: 4/23/2014