leader
: Control information at the beginning of a message or block of data. In particular, in the ARPANET, the control information on an ARPANET message at the host-IMP interface.

left sequence
: This is the next sequence number to be acknowledged by the data receiving TCP (or the lowest currently unacknowledged sequence number) and is sometimes referred to as the left edge of the send window.

local packet
: The unit of transmission within a local network.

module
: An implementation, usually in software, of a protocol or other procedure.

MSL
: Maximum Segment Lifetime, the time a TCP segment can exist in the internetwork system. Arbitrarily defined to be 2 minutes.

octet
: An eight bit byte.

Options
: An Option field may contain several options, and each option may be several octets in length. The options are used primarily in testing situations; for example, to carry timestamps. Both the Internet Protocol and TCP provide for options fields.

packet
: A package of data with a header which may or may not be logically complete. More often a physical packaging than a logical packaging of data.

port
: The portion of a socket that specifies which logical input or output channel of a process is associated with the data.

process
: A program in execution. A source or destination of data from the point of view of the TCP or other host-to-host protocol.

PUSH
: A control bit occupying no sequence space, indicating that this segment contains data that must be pushed through to the receiving user.

RCV.NXT
: receive next sequence number

RCV.UP
: receive urgent pointer

RCV.WND
: receive window

receive next sequence number
: This is the next sequence number the local TCP is expecting to receive.

receive window
: This represents the sequence numbers the local (receiving) TCP is willing to receive. Thus, the local TCP considers that segments overlapping the range RCV.NXT to RCV.NXT + RCV.WND - 1 carry acceptable data or control. Segments containing sequence numbers entirely outside of this range are considered duplicates and discarded.

RST
: A control bit (reset), occupying no sequence space, indicating that the receiver should delete the connection without further interaction. The receiver can determine, based on the sequence number and acknowledgment fields of the incoming segment, whether it should honor the reset command or ignore it. In no case does receipt of a segment containing RST give rise to a RST in response.

rise to a RST in response.

RTP
: Real Time Protocol: A host-to-host protocol for communication of time critical information.

SEG.ACK
: segment acknowledgment

SEG.LEN
: segment length

SEG.PRC
: segment precedence value

SEG.SEQ
: segment sequence

SEG.UP
: segment urgent pointer field

SEG.WND
: segment window field

segment
: A logical unit of data, in particular a TCP segment is the unit of data transfered between a pair of TCP modules.

segment acknowledgment
: The sequence number in the acknowledgment field of the arriving segment.

segment length
: The amount of sequence number space occupied by a segment, including any controls which occupy sequence space.

segment sequence
: The number in the sequence field of the arriving segment.

send sequence
: This is the next sequence number the local (sending) TCP will use on the connection. It is initially selected from an initial sequence number curve (ISN) and is incremented for each octet of data or sequenced control transmitted.

send window
: This represents the sequence numbers which the remote (receiving) TCP is willing to receive. It is the value of the window field specified in segments from the remote (data receiving) TCP. The range of new sequence numbers which may be emitted by a TCP lies between SND.NXT and SND.UNA + SND.WND - 1. (Retransmissions of sequence numbers between SND.UNA and SND.NXT are expected, of course.)

SND.NXT
: send sequence

SND.UNA
: left sequence

SND.UP
: send urgent pointer

SND.WL1
: segment sequence number at last window update

SND.WL2
: segment acknowledgment number at last window update

SND.WND
: send window

socket
: An address which specifically includes a port identifier, that is, the concatenation of an Internet Address with a TCP port.

Source Address
: The source address, usually the network and host identifiers.

SYN
: A control bit in the incoming segment, occupying one sequence number, used at the initiation of a connection, to indicate where the sequence numbering will start.

TCB
: Transmission control block, the data structure that records the state of a connection.

TCB.PRC
: The precedence of the connection.

TCP
: Transmission Control Protocol: A host-to-host protocol for reliable communication in internetwork environments.

TOS
: Type of Service, an Internet Protocol field.

Type of Service
: An Internet Protocol field which indicates the type of service for this internet fragment.

URG
: A control bit (urgent), occupying no sequence space, used to indicate that the receiving user should be notified to do urgent processing as long as there is data to be consumed with sequence numbers less than the value indicated in the urgent pointer.

urgent pointer
: A control field meaningful only when the URG bit is on. This field communicates the value of the urgent pointer which indicates the data octet associated with the sending user's urgent call.

REFERENCES

[1] Cerf, V., and R. Kahn, "A Protocol for Packet Network Intercommunication", IEEE Transactions on Communications, Vol. COM-22, No. 5, pp 637-648, May 1974.

[2] Postel, J. (ed.), "Internet Protocol - DARPA Internet Program Protocol Specification", RFC 791, USC/Information Sciences Institute, September 1981.

[3] Dalal, Y. and C. Sunshine, "Connection Management in Transport Protocols", Computer Networks, Vol. 2, No. 6, pp. 454-473, December 1978.

[4] Postel, J., "Assigned Numbers", RFC 790, USC/Information Sciences Institute, September 1981.

Html markup produced by rfcmarkup 1.44, available from http://tools.ietf.org/tools/rfcmarkup/

https://web.archive.org/web/20140102143305/http://phoneboy.net/

INTERNET ARCHIVE WayBackMachine http://phoneboy.net/ Go JUN JAN FEB 02 2005 2014 2015 About this capture
29 captures 31 May 2002 - 2 Jan 2014
POSTHAVEN Login

PhoneBoy's Security Theater

Views on Information Security from the guy who brought you ye olde PhoneBoy FireWall-1 FAQ

About PhoneBoy
PhoneBoy on app.net
PhoneBoy on Twitter
PhoneBoy on Google+
PhoneBoy on LinkedIn

Dameon Welch-Abernathy



Parent, Writer, Podcaster, Coffee Achiever, VoIP/Telco Curious, C-List Information Security Celebrity, and Mobile Phone Connoisseur residing in Gig Harbor, WA, USA.

You might know him better as PhoneBoy.

Subscribe by email »
We'll email you when there are new posts here

Tags
check point 26
nokia 9
wifi 6
mobile phones 6
iskoot 5
social networking 5
byod 5
skype 4
facebook 4
voip 3
See all 66 tags »

Sites I Like
The PhoneBoy Blog
PhoneBoy's Personal Blog

Blast from the CHKP Past: Can't Talk to Translated IP from Internal Net

It's pretty obvious from looking through the number of 404s I'm seeing in Google's Webmaster tools that a lot of pages still link to old stuff I wrote about Check Point FireWall-1. I'm actually trying to "fix" these 404s now by resurrecting some of the old content. Not updating it, of course, but at least making the links point to something semi-useful, if historical.

This is one of those articles, obviously not at it's original URL, but the original URLs will point here. What amazes me about this particular article is that it's still relevant today as NAT really hasn't fundamentally changed in the Check Point products for some time. The basic concepts are still the same, too, and other than the implementation details, is probably relevant for other security products, too.

Bottom line: NAT only works if the firewall is in the path of the communication. How do you know? Follow the bouncing packet, otherwise known as Troubleshooting 101.

Hit the break to see this old FAQ in all its ASCII network mapped glory.

Read more »

Upvote 0 Tweet

0 responses // Posted about 1 month ago

The TSA and A Lesson in Data Loss Prevention

From PhoneBoy Speaks Ep 305: Threat? What Threat?

> In sealed court documents accidentally leaked on a US Federal government website, the US government basically admits that there has been no attempted domestic hijackings of any kind in the 12 years since 9/11. Furthermore, at least as of mid-2011, terrorist threat groups present in the Homeland are not known to be actively plotting against civil aviation targets or airports.

It gets better. Jonathan Corbett, the guy who has been challenging the feds on the constitutionality and the effectiveness of the TSA in the courts, was told by the US Justice Department to take down his comments about a sealed document he wasn't allowed to talk about, but the government themselves posted the unredacted version on their site and other sites made it public.

The same is true for Corbett's comments about those documents, the Justice Department asked him to remove from his site, but they apparently forgot to tell Google as it was still in their cache!

This is a clear demonstration of what can happen if confidential data inadvertently leaves your organization. Clearly this unredacted, sealed legal brief should have never been made public. Thankfully, in this case, it was, but surely some folks in the US Government weren't happy with this lapse. Neither would your employer if it's your company's secret plans for world domination that got leaked.

Likewise, if you inadvertently leak information on your own website, or someone else does, even if you can manage to get it taken down, Google takes a while to forget it saw it. The rest of the Internet won't necessarily

forget, though. Ever.

So what are your plans for Data Loss Prevention in your organization? Are you even employing any DLP technology? Is it actually catching real incidents of data loss or is everyone going around it?

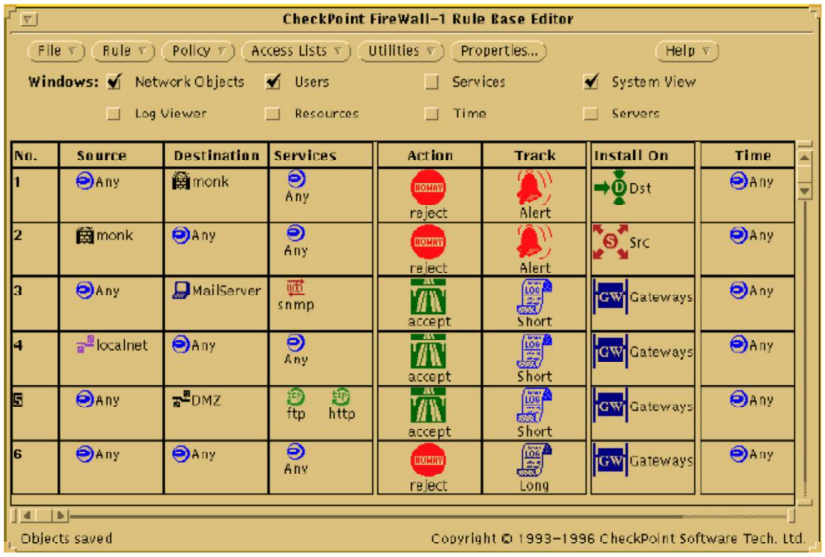
I'm not saying DLP is a panacea or 100% effective, but if you're not doing it, then you don't have any idea where your corporate information might end up.

Upvote 0 Tweet

0 responses // Posted 3 months ago

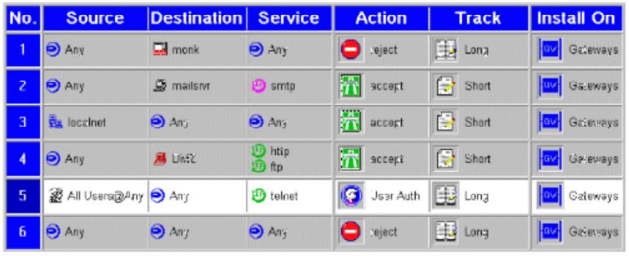
FireWall-1 User Interface from 3.0

If you ran Check Point FireWall-1 on SunOS or Solaris, you probably remember this screen:



This is a screen capture from fwui, the management interface for FireWall-1. Actually FireWall-1 2.0 and 2.1 looked like this too.

Meanwhile if you ran the management interface on Windows, you were presented with something like this:



You could actually run the firewall on Windows NT as of 2.1, though it took until 2.1c until it was reasonably stable.

Actually you could run something that looked like the Windows UI on Solaris with Motif, which Check Point charged extra for. Eventually the Motif and the OpenLook GUI were deprecated and what we now refer to as SmartDashboad only runs on Windows.

And, of course, there are far more GUI clients these days--about a dozen or so if I remember correctly. But then again, the product does so much more today than it did back in the mid 1990s.

And yes, I remember those days quiet fondly.

Upvote 0 Tweet

2 responses // Posted 5 months ago

Blast from the CHKP Past: Can't Get Putkeys to Work

For those of you who never had to work with Check Point FireWall-1 4.1 and earlier, you're lucky you likely never EVER had to use putkeys.

The fw putkey was used to establish authentication between the Management and Firewall modules. The problem was: the authentication would frequently break. Especially in larger, distributed environments. Often for reasons that no one outside of a few developers in Tel Aviv never fully understood.

The eventual replacement for fw putkey was SIC, which was added in FireWall-1 NG (5.0). It is based on certificates and is way easier to set up. It's also far less prone to random breakage.

The following classic article is presented for nostalgia purposes only. Hopefully no one in their right mind still needs this article, which was very popular on my FireWall-1 FAQ back in the day. It was the collective wisdom of my peers and my own experience as of around 2000 or so.

Read more »

Upvote 1 Tweet

2 responses // Posted 5 months ago

Moving The Security Theater Elsewhere

I decided to move PhoneBoy's Security Theater off of Wordpress onto Posthaven.

On the plus side, it's one less instance of Wordpress to maintain. On the minus side, I had to copy/paste the old articles in since there is no way to import Wordpress as of yet. But it was under 100 articles and it was kind of nice to see my thoughts on security from the last several years again.

The reality is, the threats haven't changed. We've had to evolve the tools in order to address increasingly complex threats. You can look at Check Point's own product evolution to get a sense of that.

Also, the basics haven't changed. A lot of security risks can be sufficiently mitigated by properly segmenting your networks, using sufficiently complex passwords that are unique, proper monitoring of the logs of your security devices, and keeping your software up-to-date with the latest security patches.

Tags administrivia

Upvote 0 Tweet

0 responses // Posted 5 months ago

Fun with Compliance

Earlier this week, I hung out with Jeremy Kaye, one of our in-house compliance experts at Check Point:

http://www.youtube.com/embed/uvL6HdlrW08

While I've been doing InfoSec for a while, or at least working in companies that sell InfoSec products, compliance isn't something I've had a ton of direct experience with. Sure, Check Point customers used our products to help meet various compliance regulations, but until Check Point acquired DynaSec in 2011, there

wasn't a team inside Check Point dedicated to this topic.

While we had some technical challenges with the Google+ Hangout itself (and it was the first one we did at Check Point), I think the conversation with Jeremy went fairly well. The questions I asked where ones I've always wanted answers to. Like, what good is compliance? Why does it seem like compliance is in the eye of the auditor? Why so many regulations anyway?

The big takeaway for me from this conversation is that security should drive your compliance efforts, not the other way around. Because chances are, if you have a strong information security program in place already, compliance is pretty straightforward, no matter which regulations you have to comply with.

Tags compliance

Upvote 0 Tweet

0 responses // Posted 6 months ago

Check Point 600 Appliance: Big Security for Small Business

Ok, this is a completely shameless plug for my employer. But it's really big. And really small at the same time. And my take on it, which wasn't cleared with the marketing folks, and thus my, albeit biased, opinion.

The Check Point 600 Appliance, which was announced today at Interop, represents Check Point's refreshed entry into the SMB Security space. It provides the same security functionality you'd find in Check Point's larger appliances in something that fits into an SMB--both in terms of form factor and price. This includes Check Point's award-winning IPS, App Control, URL Filtering, Anti-Virus, Anti-Spam, VPN, oh and don't forget the firewall :)

If you're familiar with the SG80, which Check Point launched a couple years back, the new 600 Appliance looks a bit like that, though the internals are slightly different from the SG80. There are standard USB ports, Express Card and SD-card slots in the 600 as well as optional WiFi and ADSL ports. It also includes a revamped Web Interface that incorporates functionality from the UTM-1 EDGE and Safe@ appliances allowing full management of the security policy across all Software Blades.

Under the hood? It's nearly the same code that runs in the larger Check Point appliances--Check Point R75.20 running Embedded Gaia, to be exact. When you SSH or serial console into the appliance, you are presented with clish, which functions similar to how it does on one of the larger appliances. You can also drop into Expert mode for more advanced debugging, which again, works very similar to how its done on the larger gateways.

The main differences between the 600 and the Check Point 1100 Appliance, which was announced a few weeks ago are:

- Lower price: List price of a 600 is roughly $200 cheaper than the comparable 1100 model.
- Chassis color: Bright orange, like the old Safe@ boxes.
- Central Management: While the 1100 can be centrally managed with standard R75.46 or R76 management (standalone or Provider-1), the 600 can only be centrally managed by Check Point Cloud-Managed Security service.

In any case, I am truly excited about this as finally, SMBs can finally get the same Enterprise-grade security that the Fortune 100 relies on for a fraction of the cost--starting at $399.

Check Point's SMB Portal has information about the new appliances as well as how to acquire them.

Tags check point smb

Upvote 0 Tweet

0 responses // Posted 8 months ago

Check Point 2013 Security Report

When I was in Israel at the end of 2012, I was talking with the folks putting the finishing touches on the Check Point 2013 Security Report. Of course, since then, the report has been formally released and you can now read it for yourself. Here's a video preview of what you'll find in it:



Some of the data gathered for this report was related to the 3D Security Reports Check Point generated for customers during 2012 where we took a Security Gateway and either ran it in-line (in bridge mode) or plugged it into a mirror port on a customer's switch. It's worth pointing out that, in many cases, *a competitive security solution was already in place* and the Check Point Security Gateways were seeing stuff the other solutions were missing.

Other data for this report also came from SensorNet, ThreatCloud, and results from our Endpoint Security Best Practices Report, which is a great way to find out if your Windows PC is configured according to our Best Practices.

The most surprising statistics?

- 63% of the organizations surveyed had at least one malicious bot in their network.
- 43% of the organizations surveyed had traffic to/from an anonymizer service.

Of course, if you're knee deep in the security space, 0% of this is news to you.

Tags check point

Upvote 0 Tweet

0 responses // Posted 9 months ago

How to Not Be Like Burger King. Or Jeep.

On today's episode of PhoneBoy Speaks, I discuss how to prevent your Twitter account from being hacked like Burger King's account was. And today (after I recorded this episode), Jeep's Twitter account was also hacked. Of course, I can only do so much in a 5 minute podcast, and the topic itself of choosing strong passwords--and getting users to actually do it--has been covered ad-infinitum elsewhere.

The fact is, passwords are not very secure. To be secure, they must be both long (number of characters) and high-entropy (more random, the better). Humans, as a lot, are not able to remember passwords that meet both of these requirements, so they cheat. They either write the passwords down, they use password management tools like LastPass or 1Password, or they just choose stupid passwords--usually the latter.

The best compromise I've seen is actually the Password Haystacks method that Steve Gibson came up with. All other things being equal, as long as you use all 4 different types of characters in your password, length wins. Because when it comes to guessing passwords, there is no such thing as "close."

Of course, if the password itself can't be guessed, surely you can compromise the password reset process, as was done with Mat Honan's widely publicized pwnage. Hopefully we can strengthen that too, but companies--

especially ones that cater to non technical people--rarely err on the side of secure.

Tags social networking passwords

Upvote 0 Tweet

0 responses // Posted 11 months ago

Securing Data in the Cloud

On my podcast PhoneBoy Speaks today, I discussed (very briefly) the idea of doing information security in the cloud. Surely, I could talk and write volumes on the subject. I've even given presentations on the subject.

The reality is, virtualization changes the game in so many ways that it's hard to know where to begin. That said, my view starts with the most basic question: what is it we're ultimately trying to protect?

The good news is that the answer is still the same, regardless of whether physical servers on your premises are involved or some cloud services provider is: it's the data. Your job in information security is to ensure the Confidentiality, Integrity, and Availability of data to prevent Disclosure, Alteration, or Destruction of said data.

The bad news: the cloud makes this job a lot harder. The reality of bring your own device (BYOD) also makes this harder for much the same reason--less opportunities to inject the necessary controls to ensure data doesn't go where it's not supposed to.

Of course, it's not just about protecting the data. That part is actually pretty easy. Protecting in a way that allows it to be used in a convenient way, now that's a lot harder.

Tags cloud byod

Upvote 0 Tweet

0 responses // Posted 11 months ago

EXHIBIT B

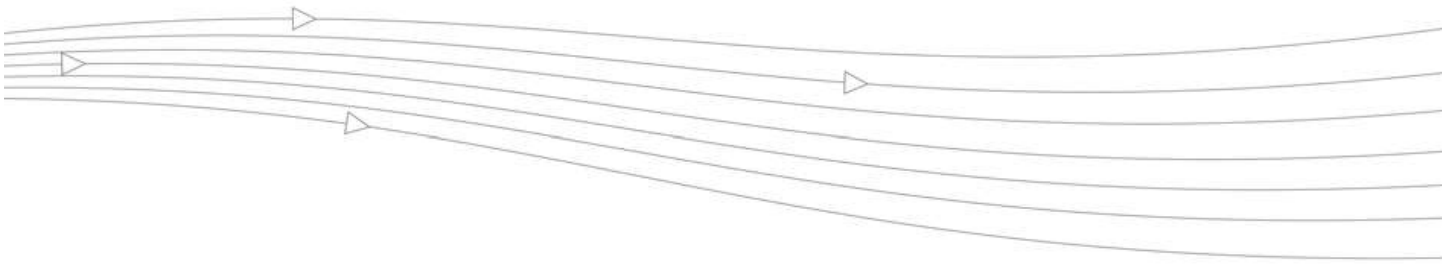
https://web.archive.org/web/20100821022839/http://www.sonicwall.com:80/downloads/SonicWALL_ViewPoint_6_0_Admin_Guide.pdf

SonicWALL
Reporting Solutions

REPORTING | **SonicWALL ViewPoint**

SonicWALL ViewPoint 6.0 Administrator's Guide

SONICWALL®



SonicWALL ViewPoint Administrator's Guide

Version 6.0

SonicWALL, Inc.
2001 Logic Drive
San Jose, CA 95124-3452
Phone: +1.408.745.9600
Fax: +1.408.745.9300
E-mail: info@sonicwall.com

Keysight, EX-1030
Page 161

Copyright Notice

© 2010 SonicWALL, Inc.

All rights reserved.

Under the copyright laws, this manual or the software described within, can not be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. This exception does not allow copies to be made for others, whether or not sold, but all of the material purchased (with all backup copies) can be sold, given, or loaned to another person. Under the law, copying includes translating into another language or format.

Specifications and descriptions subject to change without notice.

Trademarks

SonicWALL is a registered trademark of SonicWALL, Inc.

Windows XP, Windows Vista, Windows 7, Windows Server 2008, Windows Server 2003, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

Firefox is a trademark of the Mozilla Foundation.

Netscape is a registered trademark of Netscape Communications Corporation in the U.S. and other countries. Netscape Navigator and Netscape Communicator are also trademarks of Netscape Communications Corporation and may be registered outside the U.S.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the U.S. and/or other countries.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

End User Licensing Agreement For SonicWall ViewPoint

This End User Licensing Agreement (EULA) is a legal agreement between you and SonicWALL, Inc. (SonicWALL) for the SonicWALL software product identified above, which includes computer software and any and all associated media, printed materials, and online or electronic documentation (SOFTWARE PRODUCT). By opening the sealed package(s), installing, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not open the sealed package(s), install or use the SOFTWARE PRODUCT. You may however return the unopened SOFTWARE PRODUCT to your place of purchase for a full refund.

The SOFTWARE PRODUCT is licensed, not sold.

You acknowledge and agree that all right, title, and interest in and to the SOFTWARE PRODUCT, including all associated intellectual property rights, are and shall remain with SonicWALL. This EULA does not convey to you an interest in or to the SOFTWARE PRODUCT, but only a limited right of use revocable in accordance with the terms of this EULA.

- The SOFTWARE PRODUCT is licensed as a single product and can only be used as such.
- You may also store or install a copy of the SOFTWARE PRODUCT on a storage device, such as a network server, used only to install or run the SOFTWARE PRODUCT on your other computers over an internal network.
- You may not resell, or otherwise transfer for value, rent, lease, or lend the SOFTWARE PRODUCT.
- The SOFTWARE PRODUCT is trade secret or confidential information of SonicWALL or its licensors. You shall take appropriate action to protect the confidentiality of the SOFTWARE PRODUCT. You shall not reverse-engineer, de-compile, or disassemble the SOFTWARE PRODUCT, in whole or in part. The provisions of this section will survive the termination of this EULA.
- You agree and certify that neither the SOFTWARE PRODUCT nor any other technical data received from SonicWALL, nor the direct product thereof, will be exported outside the United States except as permitted by

the laws and regulations of the United States, which may require U.S. Government export approval/licensing. Failure to strictly comply with this provision shall automatically invalidate this License.

License

SonicWALL grants you a non-exclusive license to use the SOFTWARE PRODUCT for a number of SonicWALL eligible products. This number is specified and shipped with the SOFTWARE PRODUCT. Support for additional SonicWALL eligible products is subject to a separate upgrade license.

Upgrades

If the SOFTWARE PRODUCT is labeled as an upgrade, you must be properly licensed to use a product identified by SonicWALL as being eligible for the upgrade in order to use the SOFTWARE PRODUCT. A SOFTWARE PRODUCT labeled as an upgrade replaces and/or supplements the product that formed the basis for your eligibility for the upgrade. You may use the resulting upgraded product only in accordance with the terms of this EULA. If the SOFTWARE PRODUCT is an upgrade of a component of a package of software programs that you licensed as a single product, the SOFTWARE PRODUCT may be used and transferred only as part of that single product package and may not be separated for use on more than one computer.

Support Services

SonicWALL may provide you with support services related to the SOFTWARE PRODUCT (“Support Services”). Use of Support Services is governed by the SonicWALL policies and programs described in the user manual, in “online” documentation, and/or in other SonicWALL-provided materials. Any supplemental software code provided to you as part of the Support Services shall be considered part of the SOFTWARE PRODUCT and subject to terms and conditions of this EULA. With respect to technical information you provide to SonicWALL as part of the Support Services, SonicWALL may use such information for its business purposes, including for product support and development. SonicWALL shall not utilize such technical information in a form that identifies its source.

Ownership

As between the parties, SonicWALL retains all title to, ownership of, and all proprietary rights with respect to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and ‘applets” incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT. The SOFTWARE PRODUCT is protected by copyrights laws and international treaty provisions. The SOFTWARE PRODUCT is licensed, not sold. This EULA does not convey to you an interest in or to the SOFTWARE PRODUCT, but only a limited right of use revocable in accordance with the terms of this EULA.

U.S. Government Restricted Rights

If you are acquiring the Software including accompanying documentation on behalf of the U.S. Government, the following provisions apply. If the Software is supplied to the Department of Defense (“DoD”), the Software is subject to “Restricted Rights”, as that term is defined in the DOD Supplement to the Federal Acquisition Regulations (“DFAR”) in paragraph 252.227 7013(c) (1). If the Software is supplied to any unit or agency of the United States Government other than DOD, the Government’s rights in the Software will be as defined in paragraph 52.227 19(c) (2) of the Federal Acquisition Regulations (“FAR”). Use, duplication, reproduction or disclosure by the Government is subject to such restrictions or successor provisions. Contractor/Manufacturer is: SonicWALL, Inc. 2001 Logic Drive, San Jose, CA 95124-3452, USA.

Exports License

Licensee will comply with, and will, at SonicWALL's request, demonstrate such compliance with all applicable export laws, restrictions, and regulations of the U.S. Department of Commerce, the U.S. Department of Treasury and any other any U.S. or foreign agency or authority. Licensee will not export or re-export, or allow the export or re-export of any product, technology or information it obtains or learns pursuant to this Agreement (or any direct product thereof) in violation of any such law, restriction or regulation, including, without limitation, export or re-export to Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria or any other country subject to applicable U.S. trade embargoes or restrictions, or to any party on the U.S. Export Administration Table of Denial Orders or the U.S. Department of Treasury List of Specially Designated Nationals, or to any other prohibited destination or person pursuant to U.S. law, regulations or other provisions.

Miscellaneous

This EULA represents the entire agreement concerning the subject matter hereof between the parties and supercedes all prior agreements and representations between them. It may be amended only in writing executed by both parties. This EULA shall be governed by and construed under the laws of the State of California as if entirely performed within the State and without regard for conflicts of laws. Should any term of this EULA be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms hereof. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

Termination

This EULA is effective upon your opening of the sealed package(s), installing or otherwise using the SOFTWARE PRODUCT, and shall continue until terminated. Without prejudice to any other rights, SonicWALL may terminate this EULA if you fail to comply with the terms and conditions of this EULA. SonicWALL reserves the right to terminate this EULA five (5) years after the SOFTWARE PRODUCT is issued to Licensee. In event of termination, you agree to return or destroy the SOFTWARE PRODUCT (including all related documents and components items as defined above) and any and all copies of same.

Limited Warranty

SonicWALL warrants that a) the software product will perform substantially in accordance with the accompanying written materials for a period of ninety (90) days from the date of purchase, and b) any support services provided by SonicWALL shall be substantially as described in applicable written materials provided to you by SonicWALL. Any implied warranties on the software product are limited to ninety (90) days. Some states and jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

Customer Remedies

SonicWALL's and its suppliers' entire liability and your exclusive remedy shall be, at SonicWALL's option, either a) return of the price paid, or b) repair or replacement of the SOFTWARE PRODUCT that does not meet SonicWALL's Limited Warranty and which is returned to SonicWALL with a copy of your receipt. This Limited Warranty is void if failure of the SOFTWARE PRODUCT has resulted from accident, abuse, or misapplication. Any replacement SOFTWARE PRODUCT shall be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer. Outside of the United States, neither these remedies nor any product Support Services offered by SonicWALL are available without proof of purchase from an authorized SonicWALL international reseller or distributor.

No Other Warranties

To the maximum extent permitted by applicable law, SonicWALL and its suppliers/licensors disclaim all other warranties and conditions, either express or implied, including, but not limited to, implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement, with regard to the SOFTWARE PRODUCT, and the provision of or failure to provide support services. This limited warranty gives you specific legal rights. You may have others, which vary from state/jurisdiction to state/jurisdiction.

Limitation of Liability

Except for the warranties provided hereunder, to the maximum extent permitted by applicable law, in no event shall SonicWALL or its suppliers/licensors be liable for any special, incidental, indirect, or consequential damages for lost business profits, business interruption, loss of business information,) arising out of the use of or inability to use the SOFTWARE PRODUCT or the provision of or failure to provide support services, even if SonicWALL has been advised of the possibility of such damages. In any case, SonicWALL's entire liability under any provision of this EULA shall be limited to the amount actually paid by you for the SOFTWARE PRODUCT; provided, however, if you have entered into a SonicWALL support services agreement, SonicWALL's entire liability regarding support services shall be governed by the terms of that agreement. Because some states and jurisdiction do not allow the exclusion or limitation of liability, the above limitation may not apply to you.

Manufacturer is SonicWALL, Inc. with headquarters located at 2001 Logic Drive, San Jose, CA 95124-3452, USA.

Keysight, EX-1030
Page 165

Keysight, EX-1030
Page 166

Table of Contents

Table of Contents 1

Chapter 1: Introduction to SonicWALL ViewPoint 9

- SonicWALL ViewPoint Overview 9
- SonicWALL ViewPoint Installation 10
  - License and Registration Requirements 10
- Accessing the Correct Management Interface 11
  - Switching Between Management Interfaces 12
  - Tips and Tutorials 12
- Navigating the ViewPoint User Interface 13
  - UTM Panel 13
  - SSL-VPN Panel 15
  - Console Panel 16
- ViewPoint Views and Status 17
- Using the ViewPoint TreeControl Menu 20
- About Signed Applets in SonicWALL ViewPoint 21

Chapter 2: Using the UMH System Interface 23

- Overview of the UMH System Interface 24
  - Switching to the Application Interface 24
  - Viewing Online Help and Tips 24
  - Logging Out of the UMH System Interface 25
- Configuring UMH System Settings 25
  - Viewing System Status 26
  - Managing System Licenses 26
  - Configuring System Administration Settings 28
  - Managing System Settings 29
  - Using System Diagnostics 30
- Configuring UMH Deployment Options 31

Configuring the Deployment Role 32
Configuring Deployment Settings 34
Controlling Deployment Services 36

Chapter 3: Adding SonicWALL Appliances 37

Adding SonicWALL Appliances to SonicWALL ViewPoint 37
Adding SonicWALL Appliances 38
Modifying SonicWALL Appliance Settings 39
Deleting SonicWALL Appliances from ViewPoint 39

Chapter 4: Using the SonicToday Panel 41

Overview of the SonicToday Panel 42
Editing a Component Window 42
Adding a Component Window 44
Application Widget 44
RSS Feed 46
Adding More Pages 47
Editing and Deleting Pages 48
Other Features 49

Chapter 5: Configuring User Settings 51

Configuring General Settings 51
Configuring Reports Settings 53
Adding Web Sites to the Filter List 54
Deleting Web Sites from the Filter List 54
Adding Web Users to the Filter List 54
Deleting Web Sites from the Filter List 55

Chapter 6: Configuring Log Settings 57

Configuration 57
View Log 58

Chapter 7: Configuring Management Settings 61

Settings 61
Configuring Email Settings 62
Configuring System Debug Level 62
Enforcing Password Security 63
Synchronizing Model Codes 63
Alert Settings 64
Sessions 65
Managing Sessions 65

Keysight, EX-1030
Page 168

Database Maintenance 66
Configuring Backup Schedule and Settings 67
Backing Up a Database Immediately 68
Restoring a Database Backup 68

Chapter 8: Managing Reports in the Console Panel 71

Settings 71
Enabling Report Table Sorting 72
Controlling the Number of Appliances with Log Viewer Enabled 72
Summarizer 73
About Summary Data in Reports 73
Summarizer Settings and Summarization Interval 73
Configuring the Syslog Deletion Schedule Settings 78
Configuring Host Name Resolution 79
Email/Archive 81
Configuring Email/Archive Settings 81
Scheduled Reports 82
Management 87
Configuring Report Data Management 87

Chapter 9: Using Diagnostics 89

Summarizer Status 90

Chapter 10: Granular Event Management 97

Granular Event Management Overview 97
What is Granular Event Management? 98
How Does Granular Event Management Work? 98
Using Granular Event Management 99
About Alerts 100
Configuring Granular Event Management 101
Configuring Events on the Console Panel 101
Enabling or Disabling Alerts on the UTM Panel 107
Viewing Current Alerts 108

Chapter 11: Web Services 109

URI Basics 110
Settings 111
Status 112

Chapter 12: Using ViewPoint Help 113

Tips and Tutorials 113

About ViewPoint 114

Chapter 13: ViewPoint Reporting Features 115

ViewPoint Reporting Overview 115
Viewing ViewPoint Reports 117
Navigating ViewPoint Reporting 119
Global Views 120
Unit View 121
Using Interactive Reports 122
Searching for a Report 123
Collapsible TreeControl Pane 128
Enabling/Disabling Scheduled Reports 128
Combined Reports 128
Improved Navigation 129
Showing Domain Names in Reports 130
Managing ViewPoint Reports on the Console Panel 131

Chapter 14: Scheduling and Configuring Reports 133

Configuring Scheduled Reports 134
Viewing or Managing Scheduled Reports 134
Adding or Editing a Scheduled Report 135
Selecting Reports for Summarization 137
Configuring Inheritance for Reporting Screens 138
Configuring Data Storage Settings 139
Configuring Summarization Data for Top Usage 140
Configuring Summarization Data for Bandwidth Reports 141
Configuring Dashboard Summary Reports 142
Viewing Current Alerts 144
Scheduling PDF Compliance Reports 144
Compliance Report Overview 144
Adding a New Scheduled Compliance Report 145
Customizing Your Detailed Reports Page 149

Chapter 15: Viewing Reports 153

Managing Report Settings 154
Editing Report Settings 154
Selecting a Graphical Display 154
Setting a Date or Date Range 155
Additional Settings 156
Troubleshooting Reports 156
Viewing General Status Reports 157

Keysight, EX-1030
Page 170

Viewing Dashboard Reports 159
Viewing the Dashboard Summary Report 159
Viewing the Security Dashboard Report 162
Using Custom Reports on UTM Appliances 163
Toggling Between Split Mode and Full Mode 164
Configuring the Date and Time for Custom Reports 166
Configuring the Report Layout and Generating the Report 168
Generating the Custom Report 176
Viewing a Custom Report 177
Printing a Page or Exporting the Report as a PDF or CSV File 179
Saving the Report Template 180
Viewing Bandwidth Reports 180
Viewing the Bandwidth Summary Report 181
Viewing the Top Users of Bandwidth 183
Viewing Bandwidth Usage Over Time 185
Viewing the Top Users of Bandwidth Over Time 187
Viewing Services Reports 189
Viewing the Services Summary Report 189
Viewing Web Usage Reports 191
Viewing the Web Usage Summary Report 192
Viewing the Top Web Sites 194
Viewing the Top Users of Web Bandwidth 195
Viewing Web Usage by User 197
Viewing Web Usage By Site 199
Viewing Web Usage By Category 200
Viewing Web Usage Over Time 202
Viewing Top Sites Over Time 203
Viewing Top Users Over Time 205
Viewing Web Usage By User Over Time 207
Viewing Web Usage By Category Over Time 208
Viewing Web Filter Reports 209
Viewing the Web Filter Summary Report 210
Viewing the Web Filter Top Sites Report 212
Viewing the Top Users that Try to Access Blocked Sites 213
Viewing the Blocked Sites for Each User 215
Viewing Blocked Sites Sorted By Site 216
Viewing Blocked Sites Sorted By Category 217
Viewing Blocked Site Attempts Over Time 219
Viewing the Top Blocked Site Attempts Over Time 220
Viewing the Top Blocked Site Users Over Time 221
Viewing Blocked Sites for Each User Over Time 222

Keysight, EX-1030
Page 171

Viewing Blocked Sites By Category Over Time 223
Viewing File Transfer Protocol Reports 225
Viewing the FTP Summary Report 225
Viewing the Top FTP Sites By User 227
Viewing FTP Bandwidth Usage Over Time 228
Viewing the Top Users of FTP Bandwidth Over Time 230
Viewing Mail Usage Reports 231
Viewing the Mail Usage Summary Report 232
Viewing the Top Users of Mail Bandwidth 234
Viewing Mail Usage Over Time 235
Viewing the Top Users of Mail Bandwidth Over Time 237
Viewing VPN Usage Reports 238
Viewing the VPN Usage Summary Report 239
Viewing the Top VPN Users 241
Viewing VPN Usage Over Time 242
Viewing the Top VPN Users Over Time 243
Viewing VPN Usage By Policy 245
Viewing the Top VPN Policies Over Time 246
Viewing Hourly VPN Usage By Policy 248
Viewing the VPN Services Summary Report 249
Viewing Attacks Reports 250
Viewing the Attack Summary Report 251
Viewing the Attacks By Category 253
Viewing the Errors Report 254
Viewing Attack Reports Over Time 256
Viewing the Attacks By Category Over Time 257
Viewing Errors Over Time 258
Viewing Virus Attacks Reports 260
Viewing the Top Viruses By Attack Attempts Report 262
Viewing the Virus Attack Attempts Report 263
Viewing the Virus Attacks By User Report 265
Viewing Anti-Spyware Reports 266
Viewing a Spyware Summary 268
Viewing Spyware Attempts By Category 269
Viewing Spyware Attempts Over Time 270
Viewing Spyware Attempts By Category Over Time 272
Viewing Intrusion Prevention Reports 273
Viewing the Intrusion Prevention Summary Report 275
Viewing Intrusion Attempts By Category 276
Viewing Intrusions Over Time 278
Viewing Intrusion Reports By Category Over Time 280

Keysight, EX-1030
Page 172

Viewing Application Firewall Reports 281
Viewing the Application Firewall Summary Report 282
Viewing the Application Firewall Over Time Report 283
Viewing Application Firewall Top Applications 284
Viewing Application Firewall Top Users 285
Viewing Application Firewall Top Policies 286
Viewing Authentication Reports 287
Viewing the User Login Report 288
Viewing the Administrator Login Report 289
Viewing the Failed Login Report 289
Viewing the Log 290
Viewing the Log for a SonicWALL Appliance 291

Chapter 16: SSL-VPN Reporting 293

SSL-VPN Reporting Overview 293
What is SSL-VPN Reporting? 294
Benefits of SSL-VPN Reporting 294
How Does SSL-VPN Reporting Work? 295
Using and Configuring SSL-VPN Reporting 295
About Viewing Available SSL-VPN Report Types 295
Configuring SSL-VPN Scheduled Reports 296
Configuring SSL-VPN Summarization 297

Chapter 17: Viewing SSL-VPN Reports 299

Viewing General Status Reports 299
Viewing SSL-VPN Bandwidth Reports 301
Viewing SSL-VPN Bandwidth Summary Reports 301
Viewing SSL-VPN Top Users of Bandwidth Reports 303
Viewing SSL-VPN Bandwidth Usage Over Time Reports 304
Viewing SSL-VPN Top Users of Bandwidth Over Time Reports 306
Using SSL-VPN Custom Reports 307
Toggling Between Split Mode and Full Mode 308
Configuring the Date and Time for Custom Reports 311
Configuring the Report Layout and Generating the Report 314
Generating the Custom Report 320
Viewing a Custom Report 321
Printing a Page or Exporting the Report as a PDF or CSV File 323
Saving the Report Template 324
Viewing SSL-VPN Resources Reports 325
Viewing SSL-VPN Resources Summary Reports 325
Viewing SSL-VPN Resources Top Users Reports 327

Keysight, EX-1030
Page 173

Viewing SSL-VPN Authentication Reports 330
Viewing SSL-VPN User Login Reports 330
Viewing SSL-VPN Failed Login Reports 331
Viewing the SSL-VPN Log 332
Viewing the Log for a SSL-VPN Appliance 332

Appendix A: Installing SonicWALL ViewPoint 335

About Installing and Upgrading SonicWALL ViewPoint 336
Installing SonicWALL ViewPoint 336
Installation Overview 336
Activating SonicWALL ViewPoint on Your Appliances 340
Registering Your SonicWALL Appliance 341
Activating the ViewPoint Software on Your Appliance 341
Enabling the ViewPoint License on Your Appliance 342
Installing Universal Management Suite 342
Upgrading SonicWALL ViewPoint 5.1 to 6.0 349
Registering SonicWALL ViewPoint 351
Configuring Deployment Settings 354
Configuring Web Port Settings 354
Configuring SMTP Settings 355
Upgrading from ViewPoint to GMS 356
Enabling the GMS Free Trial from ViewPoint 357
Enabling the GMS Free Trial from the UMH Interface 359
Completing the Free Trial Upgrade 360
Configuring Appliances for GMS Management 364
Purchasing a SonicWALL GMS Upgrade 366
Miscellaneous Procedures and Troubleshooting Tips 368
Miscellaneous Procedures 368
Troubleshooting Tips 370

Appendix B: Technical Tips 373

Log Viewer 373
Real-time Syslog Viewer 375
Forwarding Syslog Data to Another Syslog Server 376
Posting ViewPoint Reporting to Another Web Server for End-User Access 377

Index 379

Keysight, EX-1030
Page 174

CHAPTER 1
Introduction to SonicWALL ViewPoint

This chapter provides an overview of SonicWALL ViewPoint and information about the user interface.

See the following sections:

- "SonicWALL ViewPoint Overview" on page 9
- "SonicWALL ViewPoint Installation" on page 10
- "Accessing the Correct Management Interface" on page 11
- "Navigating the ViewPoint User Interface" on page 13
- "ViewPoint Views and Status" on page 17
- "Using the ViewPoint TreeControl Menu" on page 20
- "About Signed Applets in SonicWALL ViewPoint" on page 21

SonicWALL ViewPoint Overview

Monitoring critical network events and activity, such as security threats, inappropriate Web use, and bandwidth levels, is an essential component of network security. SonicWALL ViewPoint Reporting complements SonicWALL's network security offerings by providing detailed and comprehensive reports of network activity.

TheViewPoint Reporting Module is a software application that creates dynamic, Web-based network reports. The ViewPoint Reporting Module generates both real-time and historical reports to offer a complete view of all activity through SonicWALL network security appliances. With ViewPoint Reporting, you can monitor network access, enhance security, and anticipate future bandwidth needs.

The ViewPoint Reporting Module:

- Displays bandwidth use by IP address and service
- Identifies inappropriate Web use
- Provides detailed reports of attacks
- Collects and aggregates system and network errors
- Shows VPN events and problems
- Presents visitor traffic to your Web site
- Provides detailed daily logs to analyze specific events.

SonicWALL ViewPoint Installation

SonicWALL ViewPoint can be installed as a fresh install or as an upgrade to SonicWALL ViewPoint 5.0 and above.

Beginning in SonicWALL ViewPoint 5.1, all software components related to SonicWALL ViewPoint and SonicWALL Global Management System (GMS), including the MySQL database, executable binary files for all services, and other necessary files, are installed using the Universal Management Suite (UMS) single-binary installer. All SonicWALL ViewPoint and SonicWALL GMS files are installed as part of the Universal Management Suite, but no distinction is made between SonicWALL ViewPoint and SonicWALL GMS during the installation. The initial installation phase takes just a few minutes for any type of installation, such as a SonicWALL ViewPoint server, a SonicWALL GMS server, a database server, or any other role.

To install the Universal Management Suite from the single binary installer, see the "Installing Universal Management Suite" section on page 342.

License and Registration Requirements

SonicWALL ViewPoint is registered and licensed from the Windows server on which it is installed. SonicWALL ViewPoint registration is performed using the SonicWALL Universal Management Host system interface.The "Registering SonicWALL ViewPoint" section on page 351 provides detailed instructions for registering and licensing SonicWALL ViewPoint on your Windows system.

On SonicWALL appliances that send reporting data to SonicWALL ViewPoint, ViewPoint is licensed and activated separately from SonicOS. MySonicWALL provides a way to associate SonicWALL appliances with the SonicWALL ViewPoint instance installed on the Windows system. Licensing your SonicWALL ViewPoint application on a SonicWALL appliance requires:

- **A MySonicWALL account**. A MySonicWALL account allows you to manage your SonicWALL products and purchase licenses for various services. Creating a MySonicWALL account is fast, simple, and free. Simply complete an online registration form directly from your SonicWALL security appliance management interface. Your MySonicWALL account is also accessible at <https://www.mysonicwall.com> from any Internet connection with a Web browser. Once you have an account, you can purchase SonicWALL ViewPoint and other licenses for your registered SonicWALL security appliances.
- **A registered SonicWALL security appliance with active Internet connection**. You need to register your SonicWALL security appliance to activate SonicWALL ViewPoint. Registering your SonicWALL security appliance is a simple procedure done directly from the management interface. Once your SonicWALL security appliance is registered, you can activate SonicWALL ViewPoint by using an activation key or by synchronizing with mysonicwall.com.

Accessing the Correct Management Interface

SonicWALL ViewPoint includes two separate management interfaces:

- **SonicWALL Universal Management Host (UMH) System Management Interface** – Used for system management of the SonicWALL ViewPoint instance, including registration and licensing, setting the admin password, creating backups, restarting the system, configuring network settings, selecting the deployment role, and configuring other system settings.
  Access the system management interface with the URL:

  http://<IP address>:<port>/appliance/

  If you are using the standard HTTP port, 80, it is not necessary to append the port number to the IP address. If you are accessing the interface from the same system on which it is installed, use the following URL:

  http://localhost/appliance/
- **SonicWALL ViewPoint Management Interface** – Used to access the SonicWALL ViewPoint application that runs on the system. This interface is used to configure and view SonicWALL ViewPoint reporting on SonicWALL appliances and for configuring SonicWALL ViewPoint administrative settings. Access the SonicWALL ViewPoint management interface with one of the following URLs:

  http://<IP address>:<port>/sgms/
  http://localhost/sgms/

Switching Between Management Interfaces

You can easily switch between the SonicWALL UMH system management interface and the SonicWALL ViewPoint application management interface.

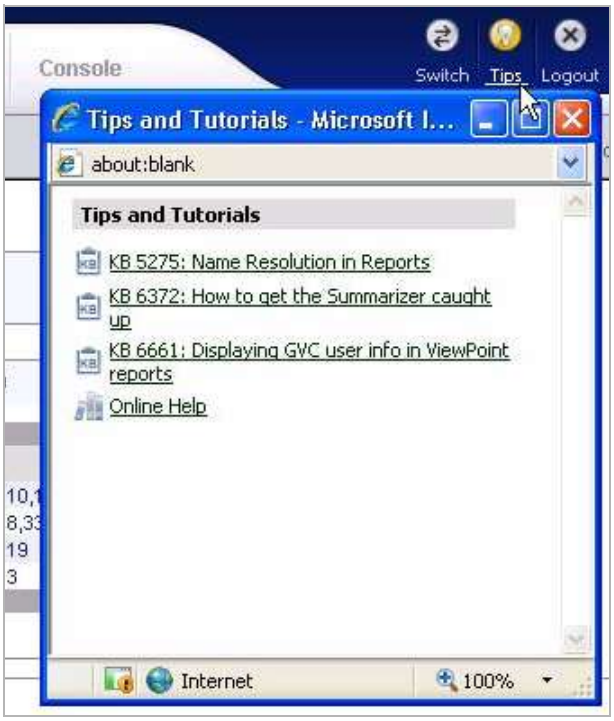
One methods is to change the URL by adding **/sgms** for the ViewPoint application interface or adding **/appliance** for the UMH interface.



A second method involves clicking the **Switch** icon. While logged into either interface, you can switch to the login page of the other interface by clicking the **Switch** button in the top right corner of the page.

Tips and Tutorials

Tips and tutorials are also available in some section of the user interface, and are denoted by a “Lightbulb” icon:



To access tips and tutorials:

1. Navigate to the page where you need help.
2. If available, click the Lightbulb icon in the upper right-hand corner of the window. Tips, tutorials, and online help are displayed for this topic.

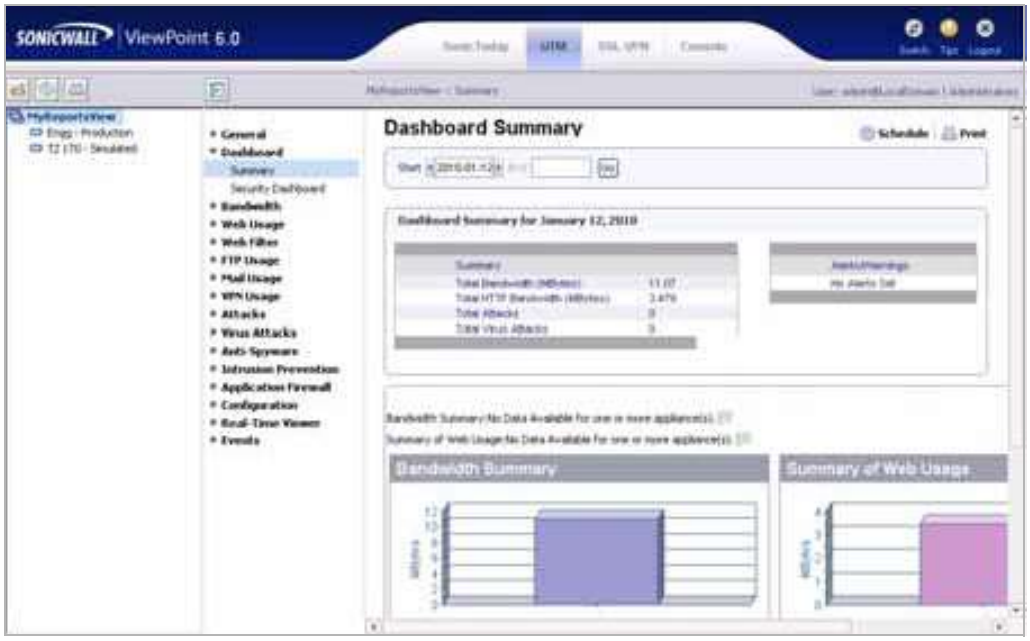
Navigating the ViewPoint User Interface

This section describes the UTM, SSL-VPN, and Console panels in the SonicWALL ViewPoint user interface. For information about the SonicToday panel, see the Using the SonicToday Panel chapter.

UTM Panel

The UTM Panel is an essential component of network security that is used to view and schedule reports about critical network events and activity, such as security threats, inappropriate Web use, and bandwidth levels.

To open the UTM Panel, click the **UTM** tab at the top of the ViewPoint user interface.



From the UTM Panel, you can view the following for connected SonicWALL appliances:

- View general unit status, license status, and syslog settings.
- View the SonicWALL security dashboard. Dashboard reports display an overview of bandwidth, uptime, intrusions and attacks, and alerts for connected SonicWALL UTM appliances. The Security Dashboard report provides data about worldwide security threats that can affect your network. The Dashboard also displays data about threats blocked by the SonicWALL security appliance.

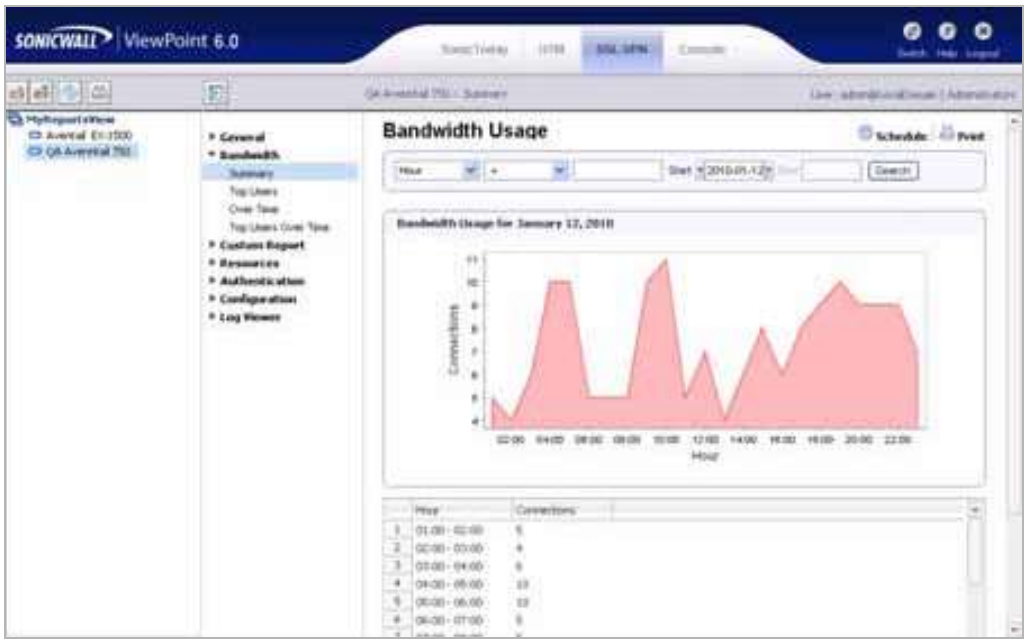
- View custom reports of Internet activity or Website filtering at the unit level. Custom reports filter raw syslog data and you can specify start and end dates or a date range such as "Week to date". You can filter by user, domain, protocol, traffic, and full URL categories, depending on the type of custom report. The search template can be saved for use again later with the same appliance.
- View general bandwidth usage. These reports include a daily bandwidth summary report, a top users of bandwidth report, and over-time summary and top users reports.
- View a services report. This report includes information about events and usage of protocols and megabytes.
- View Web bandwidth usage. These reports include a daily bandwidth summary report, a top visited sites report, a top users of Web bandwidth report, a report that contains the top sites of each user, and a weekly summary report.
- View the number of attempts that users made to access blocked websites. These reports include a daily summary report, a top blocked sites report, a top users report, a report that contains the top blocked sites of each user, and a weekly summary report.
- View file transfer protocol (FTP) bandwidth usage. These reports include a daily FTP bandwidth summary report, a top users of FTP bandwidth report, and a weekly summary report.
- View mail bandwidth usage. These reports include a daily mail summary report, a top users of mail report, and a weekly summary report.
- View VPN usage. These reports include a daily VPN summary report, a top users of VPN bandwidth report, and a weekly summary report.
- View reports on attempted attacks and errors. The attack reports include a daily attack summary report, an attack by category report, a top sources of attacks report, and a weekly attack summary report. The error reports include a daily error summary report and a weekly error summary report.
- View reports on attempted virus attacks. Virus attacks reports are available for appliances that are licensed for SonicWALL Gateway Anti-Virus. These reports include the most frequent virus attack attempts, virus attacks by top destinations, virus attacks over time, virus attacks over a period of time, and virus attacks by top destinations over time.
- View reports on attempted spyware attacks. Anti-spyware reports are available for appliances that are licensed for SonicWALL Anti-Spyware. These reports include spyware attacks by category, spyware attacks over time, and spyware attacks by category over time.

- View reports on attempted intrusion attacks. Intrusion prevention reports are available for appliances that are licensed for SonicWALL Intrusion Prevention Service. These reports include intrusion attacks by source IP address, intrusion attacks by category, intrusion attacks over time, and intrusion attacks by category over time.
- View reports on traffic triggering Application Firewall policies. Application Firewall reports are available for UTM appliances that are licensed for SonicWALL Application Firewall. These reports include summary, over time, top applications, top users, and top policies.
- View successful and unsuccessful user and administrator authentication attempts. These reports include a user authentication report, an administrator authentication report, and a failed authentication report.
- View detailed logging information. The detailed logging information contains each transaction that occurred on the SonicWALL appliance.
- View current alerts and access alert settings.

SSL-VPN Panel

The SSL-VPN panel provides access to SSL VPN appliances and is similar to the UTM panel. It is used to view and schedule reports about critical network events and activity, such as security threats, inappropriate Web use, and bandwidth levels.

To open the SSL-VPN Panel, click the **SSL-VPN** tab at the top of the ViewPoint user interface.



Keysight, EX-1030
Page 181

From the SSL-VPN Panel, you can view the following for connected SonicWALL SSL VPN appliances:

- View general unit status, license status, and syslog settings.
- View general bandwidth usage. These reports include a daily bandwidth summary report, a top users of bandwidth report, and over-time summary and top users reports.
- View custom reports of custom reports of resource activity at the unit level. Custom reports filter raw syslog data and you can specify start and end dates or a date range such as "Week to date". You can filter by user, protocol, destination IP, and source IP categories. The search template can be saved for use again later with the same appliance.
- View a resources report. This report includes information about connections and the resource used to connect, such as HTTPS or NetExtender.
- View successful and unsuccessful user authentication attempts. These reports include a user authentication report and a failed authentication report.
- View detailed logging information. The detailed logging information contains each transaction that occurred on the SonicWALL appliance.

Console Panel

The Console Panel is used to configure SonicWALL ViewPoint settings, view pending tasks, view the log, manage licenses, and configure alerts.

To open the Console Panel, click the **Console** tab at the top of the SonicWALL ViewPoint user interface.



Keysight, EX-1030
Page 182

From the Console Panel, you can do the following:

- Change the SonicWALL ViewPoint password, adjust the amount of inactive time before the user is automatically logged out of ViewPoint, and set the maximum number of rows displayed on paginated screens.
- Configure Web sites and Web users that will be excluded from Web usage reports.
- View the SonicWALL ViewPoint log and delete old log messages. The SonicWALL ViewPoint log contains information on alert notifications, failed SonicWALL ViewPoint login attempts, and other events that apply to SonicWALL ViewPoint.
- Manage SMTP settings, system email addresses, archive report settings, debug level for logs, and password security settings. You can set the schedule and server settings, and the email alert recipient schedule and preferred format.
- Manage login sessions. You can view the status of user sessions and, if necessary, end them.
- Configure report settings for sort options and maximum units with Log Viewer enabled. Enabling Log Viewer allows custom reports for the system, but is resource intensive.
- Control summarizer settings, syslog and summarized data deletion schedules, and host name resolution settings.
- Configure email archive settings and search settings for scheduled reports, and manage data archiving.
- View summarizer diagnostics, useful for capacity planning.
- Configure granular event management report settings, including threshold, schedule, and alert settings.
- Configure Web services deployment settings and view Web services status.
- View the version number, serial number, and database information for SonicWALL ViewPoint, and access links to all available tips and video tutorials.

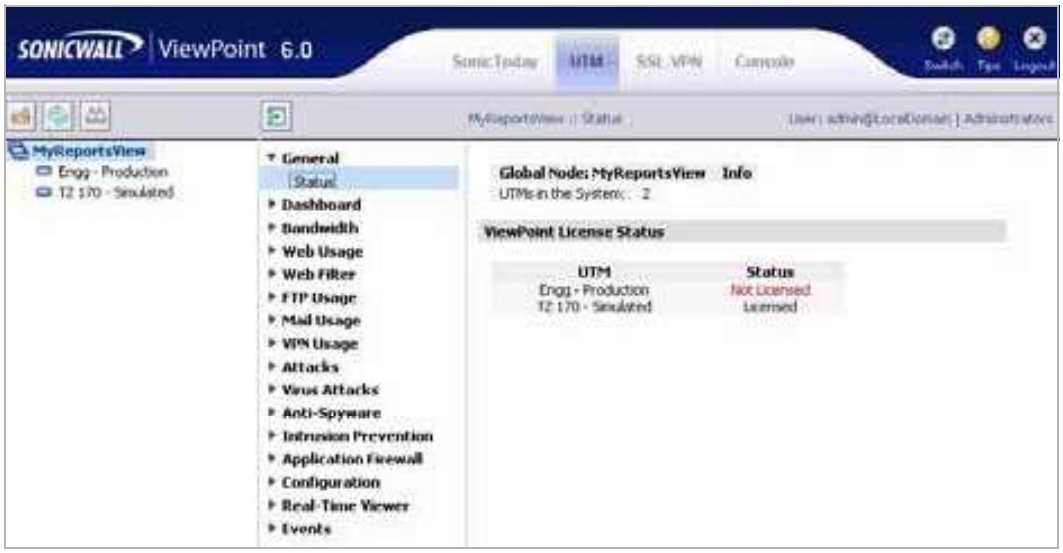
ViewPoint Views and Status

SonicWALL ViewPoint allows you to view status and reports for all appliances at once using **MyReportsView**, or for a single unit at a time with the **Unit** view.

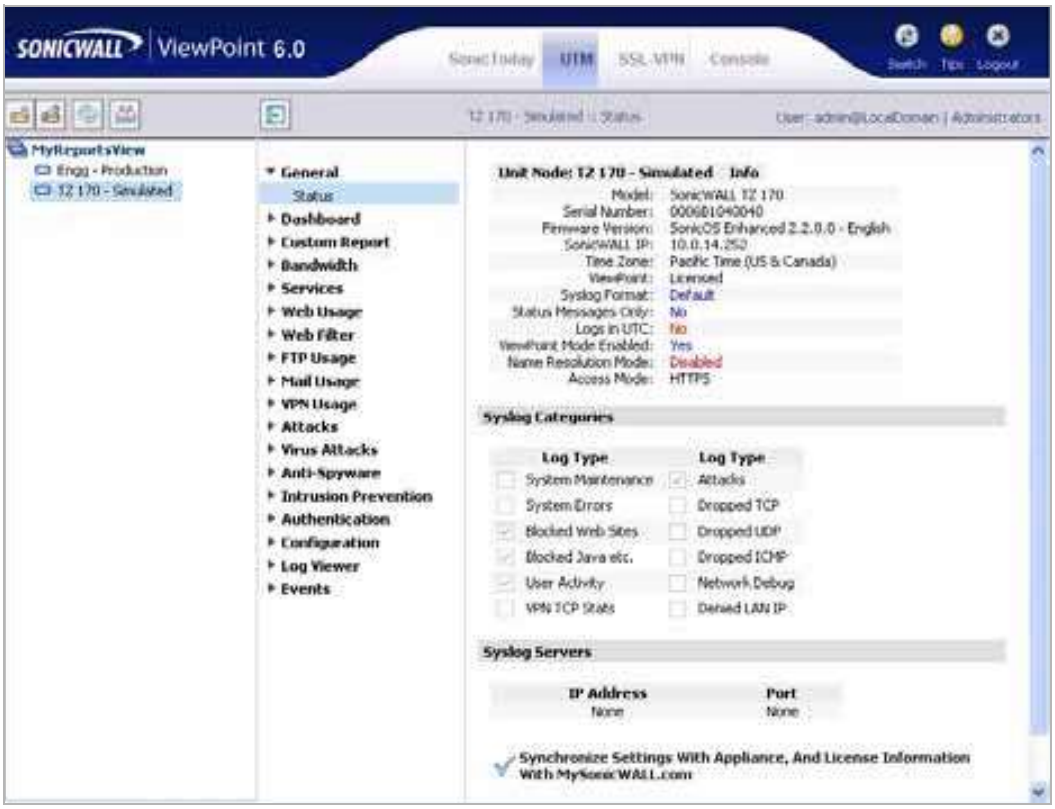
ViewPoint provides status information on the General > Status page of the UTM or SSL-VPN panel.

MyReportsView is a grouping of all the appliances you are monitoring with ViewPoint. From the MyReportsView of the UTM or SSL-VPN Panel, Summary and Over Time reports are available for all SonicWALL appliances monitored by SonicWALL ViewPoint.

To open the My Reports view, click the **MyReportsView** icon at the top of the left pane. To display the global status page, navigate to **General > Status**.



From the Unit view, reports contain detailed data for the selected SonicWALL appliance. To specify the unit view, click any unit in the left pane. To display the unit status page, navigate to **General > Status** on the **UTM** or **SSL-VPN** panel.



Using the ViewPoint TreeControl Menu

This section describes the content of the TreeControl menu within the SonicWALL ViewPoint user interface.

You can control the display of the TreeControl pane by selecting one of the appliance tabs at the top of the main window. For example, when you click the **UTM** tab, the TreeControl pane displays all the connected UTM appliance units. The two appliance tabs can display the following appliance types when ViewPoint is monitoring these device types:

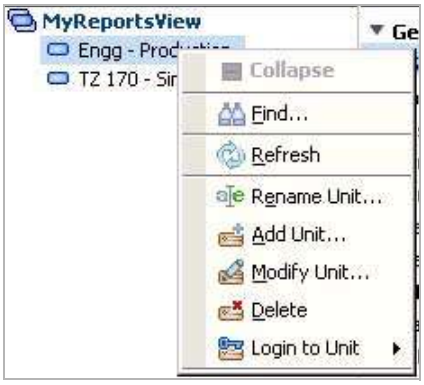
- UTM appliances
- SSL-VPN and EX-Series SRA appliances

You can hide the entire TreeControl pane by clicking the sideways arrow icon, and redisplay the pane by clicking it again. This is helpful when viewing some reports or other extra-wide screens.



To open a TreeControl appliance menu, right-click MyReportsView or a Unit icon.





The following options are available in the right-click menu:

- **Find** – Opens a Find dialog box that allows you to search for units.
- **Refresh** – Refreshes the ViewPoint UI display.
- **Rename Unit** – (unit view only) Renames the selected SonicWALL appliance.
- **Add Unit** – Add a new unit to the ViewPoint view. Requires unit IP and login information.
- **Modify Unit** – (unit view only) Change basic settings for the selected unit, including unit name, IP and login information, and serial number.

- **Delete** – Delete the selected unit
- **Login to Unit** – (unit view only) Login to the selected unit using HTTP or HTTPS protocols.

About Signed Applets in SonicWALL ViewPoint

There are a number of applets in the SonicWALL ViewPoint management interface, such as the TreeControl Applet in the leftmost pane.

Signed Applets refers to a technique for adding a digital signature to a Java applet to prove that it was not tampered with upon receipt from the signer. Signed applets can be given more privileges than ordinary applets. By default, applets have no access to system resources outside the directory from which they were launched, but a signed applet can access local system resources as allowed by the local system's security policy.

In some previous releases of ViewPoint, you were required to edit the java.policy file yourself on the client browser system in order to enable a number of applet related operations, such as Copy/Paste, Import file, Browse local folders, and HTTP/HTTPS login to the managed units from the ViewPoint management interface.

There is no need to edit the java.policy file for signed applets. When a signed applet starts up, a warning pop-up is displayed. If you want to trust the applet, click **Yes**. Copy/paste, Import and HTTP/HTTPS logins will work without any edits to the java.policy file.



Keysight, EX-1030
Page 187

Otherwise, click **No**. In this case you must manually edit the java.policy file. You can view the following technote for more information about editing the java.policy file:

Manually Configuring the java.policy File for SonicWALL GMS JRE

Keysight, EX-1030
Page 188

CHAPTER 2

Using the UMH System Interface

This chapter describes the Universal Management Host system interface, one of the two management interfaces available for SonicWALL ViewPoint.

This section includes the following subsections:

- Overview of the UMH System Interface, page 24
- Configuring UMH System Settings, page 25
- Configuring UMH Deployment Options, page 31

Overview of the UMH System Interface

The SonicWALL ViewPoint UMH system interface is used for system management of the SonicWALL ViewPoint instance, including registration and licensing, setting the admin password, configuring network and database settings, selecting the deployment role, and configuring other system settings.

When installing SonicWALL Universal Management Suite 6.0 on a host, a Web server is installed to provide the system management interface. The system interface is available by default at http://localhost/appliance/ after restarting the system.



Switching to the Application Interface



To switch between the System interface and the SonicWALL ViewPoint application interface, click the **Switch** button in the top right corner of the interface.

Viewing Online Help and Tips



To display context sensitive help for the current page, click the **Help** button in the top right corner of the interface.



The **Help** button can change to the **Tips** button if the current page has any context sensitive tips or video tutorials.

Clicking on the **Tips** button displays dynamic links for whitepapers, videos, knowledge base articles, other references, and online help.



Logging Out of the UMH System Interface



To log out of the SonicWALL ViewPoint UMH system interface, click the **Logout** button in the top right corner of the interface.

Configuring UMH System Settings

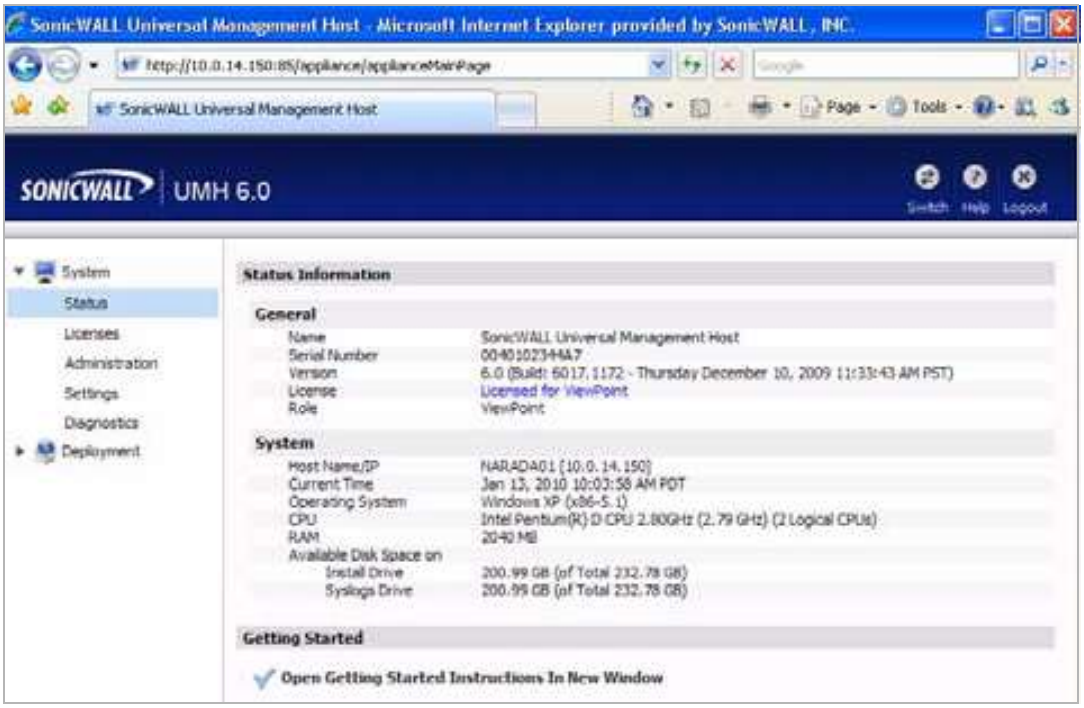
This section describes the tasks you can perform on the System pages of the SonicWALL ViewPoint UMH system interface.

See the following sections:

- Viewing System Status, page 26
- Managing System Licenses, page 26
- Configuring System Administration Settings, page 28
- Managing System Settings, page 29
- Using System Diagnostics, page 30

Viewing System Status

The System > Status page provides the general information about the installation, including the name which identifies the system as a SonicWALL Universal Management Host, the serial number of the SonicWALL ViewPoint instance, the software version, licensing status, and the system role. For SonicWALL ViewPoint, the role is always "ViewPoint."



Under System, the host name of the computer is listed, along with the time and other information about the host computer.

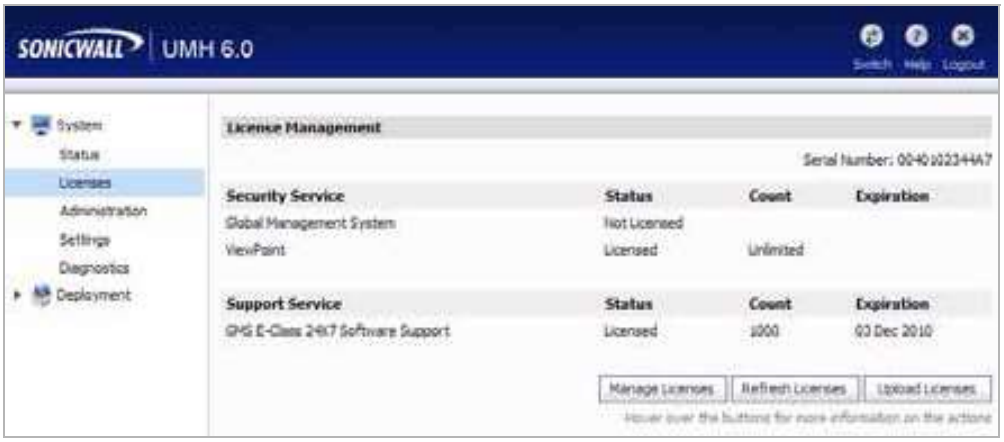
At the bottom of the page, a link is provided to access the *Getting Started Guide* which takes you to the online help table of contents.

Managing System Licenses

The System > Licenses page provides buttons for managing, refreshing, and uploading licenses. The page displays the status of ViewPoint and Global Management System licenses. The Global Management System license status will show the status of your SonicWALL GMS Free Trial, if activated. If you choose to upgrade to SonicWALL GMS, this page will show Global Management System as fully licensed.

The value in the Count column indicates the number of appliances for which this SonicWALL ViewPoint or SonicWALL GMS instance is licensed for reporting or management. For SonicWALL ViewPoint, this value is usually "unlimited", but for SonicWALL GMS, the base license is either for 10 nodes or 25 nodes, and additional node licenses can be purchased in various increments.

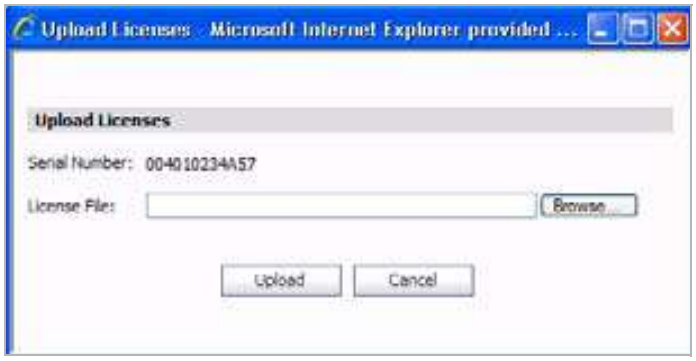
The Expiration column indicates the expiration date of the license. If no date is shown, the license is perpetual, and does not expire.



To display the MySonicWALL login page, click the **Manage Licenses** button. You can purchase licenses and obtain license keysets on MySonicWALL.

Click the **Refresh Licenses** button to refresh the license status on this page.

To upload a new license, click the **Upload Licenses** button and browse to a license file on your computer.



Keysight, EX-1030
Page 193

Configuring System Administration Settings

The System > Administration page allows you to configure the system behavior for admin login sessions.



Under Host Settings, enter the number of minutes of inactivity allowed before the session is logged out. A setting of **-1** allows an unlimited amount of inactivity without being logged out.

Under Enhanced Security Access, you can configure the number of failed login attempts before the admin account is locked out, and the number of minutes that the lockout lasts. You can also configure the number of days before the admin account password must be changed.

Under Administrator Password, you can change the administrator password for the SonicWALL ViewPoint application. Enter the current password for the system administrator (or root) account into the Current Password field, and then enter the new password into both the **New Password** and **Confirm Password** fields.

After making any changes on this page, click **Update**. To revert the fields on the page to their default settings, click **Reset**.

Managing System Settings

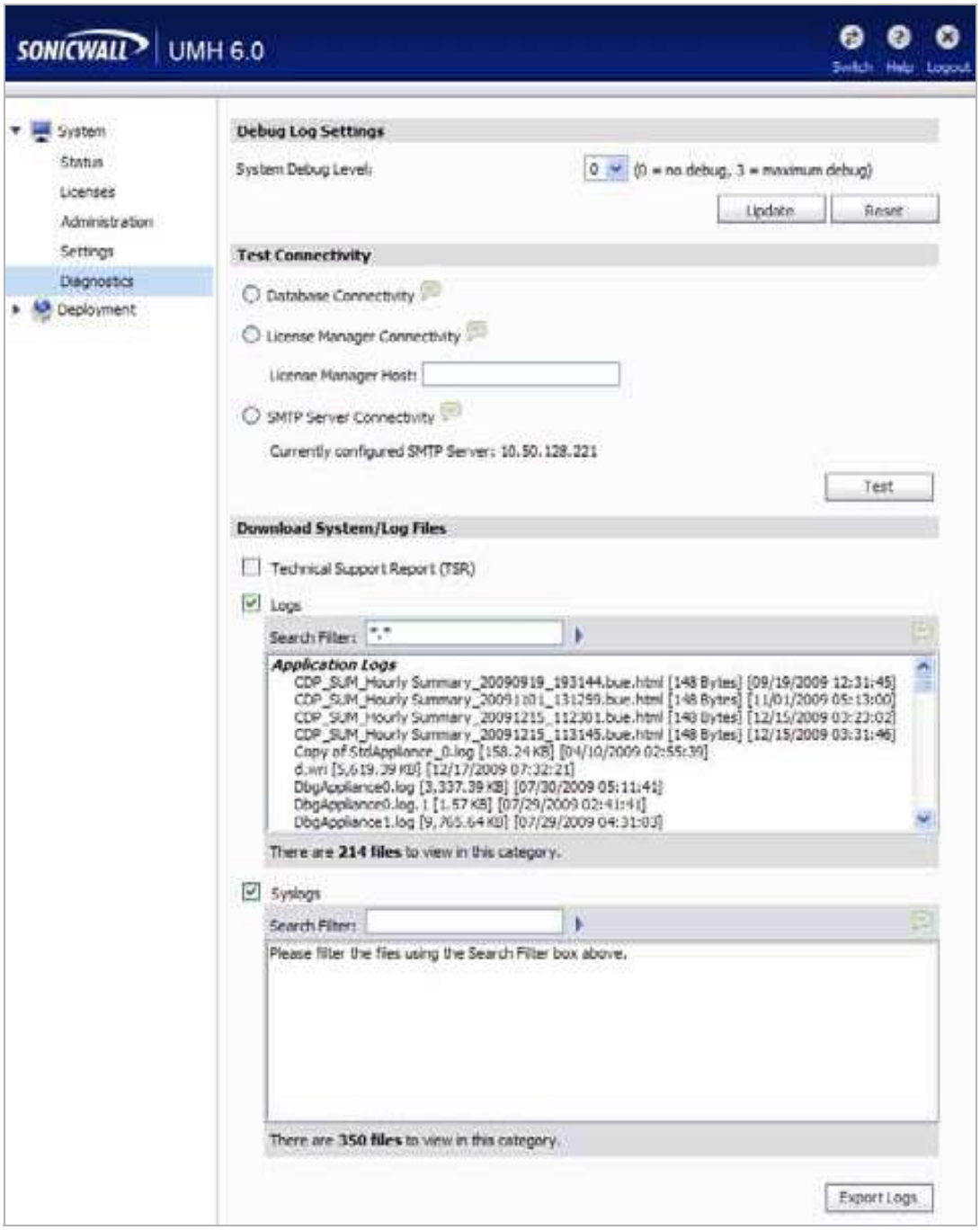
The System > Settings page provides a way to upload new SonicWALL ViewPoint software or service packs to the system. Click **Browse** to browse to the file you wish to upload, and then click **Apply**.



The page shows the current version of SonicWALL UMS, and provides a History link that displays the history of all hotfixes and firmware updates that were applied to the system.

Using System Diagnostics

The System > Diagnostics page is used to set log levels, test connectivity to servers, generate Tech Support Reports, and to search and download system log files.



Under Debug Log Settings, select the log level from the **System Debug Level** drop-down list. You can select **0** for no debug information, **1** or **2** for more, and **3** for maximum debug information.

In the Test Connectivity section, select one of the following radio buttons and then click **Test** to verify connectivity to that server:

- **Database Connectivity** – Tests connectivity to the database server configured on the Deployment > Roles page.
- **License Manager Connectivity** – Type the host name or IP address into the License Manager Host field and click Test to test connectivity to that server.
- **SMTP Server Connectivity** – Tests connectivity to the SMTP server configured on the Deployment > Settings page.

In the Download System/Log Files section, you can enter a filter, or search value, into either of the **Search Filter** fields, and then press **Enter**, to locate log entries of interest. Click the **Export Logs** button to save the log files to a file on your computer.

To generate a TSR (Technical Support Report), select the **Technical Support Report (TSR)** checkbox, and then click **Export Logs**.

Configuring UMH Deployment Options

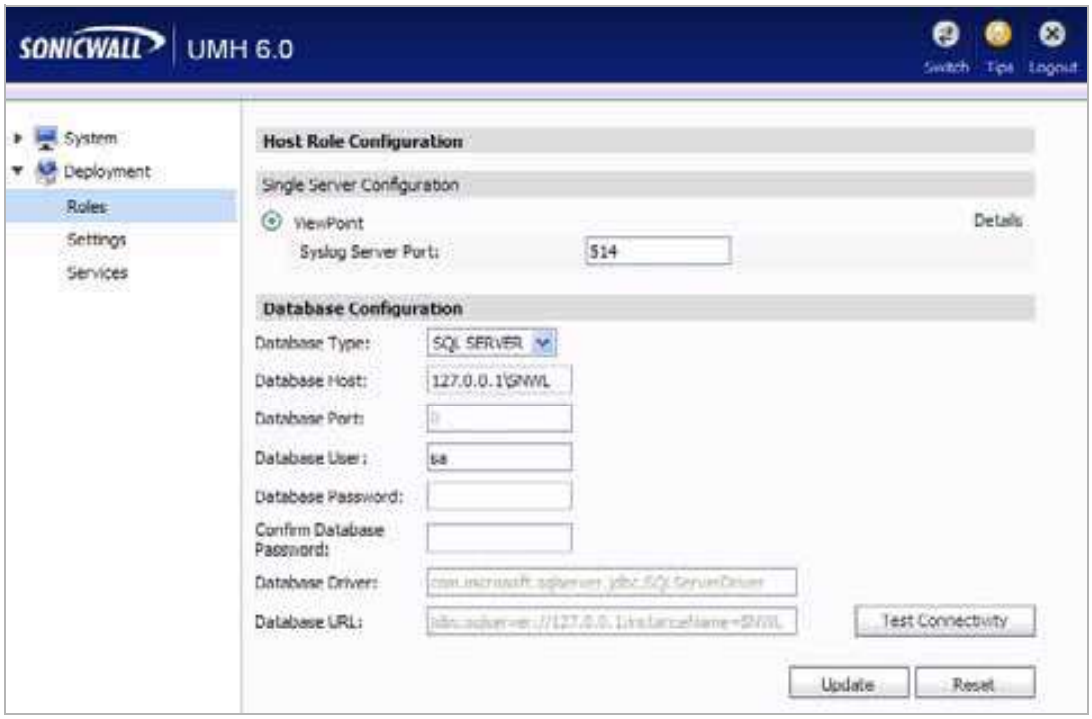
This section describes the tasks you can perform on the Deployment pages of the SonicWALL ViewPoint UMH system interface.

See the following sections:

- Configuring the Deployment Role, page 32
- Configuring Deployment Settings, page 34
- Controlling Deployment Services, page 36

Configuring the Deployment Role

In a SonicWALL ViewPoint installation, the Deployment > Roles page provides a way to configure the syslog port and the database settings, and to test database cnnectivity.



To set the syslog port, enter the port number into the **Syslog Server Port** field.

Under Database Configuration, to provide credentials with which SonicWALL ViewPoint will access the database, enter the account user name into the **Database User** field, and enter the account password into both the **Database Password** and **Confirm Database Password** fields.

To test connectivity to the database server, click **Test Connectivity**. A popup will display the status.

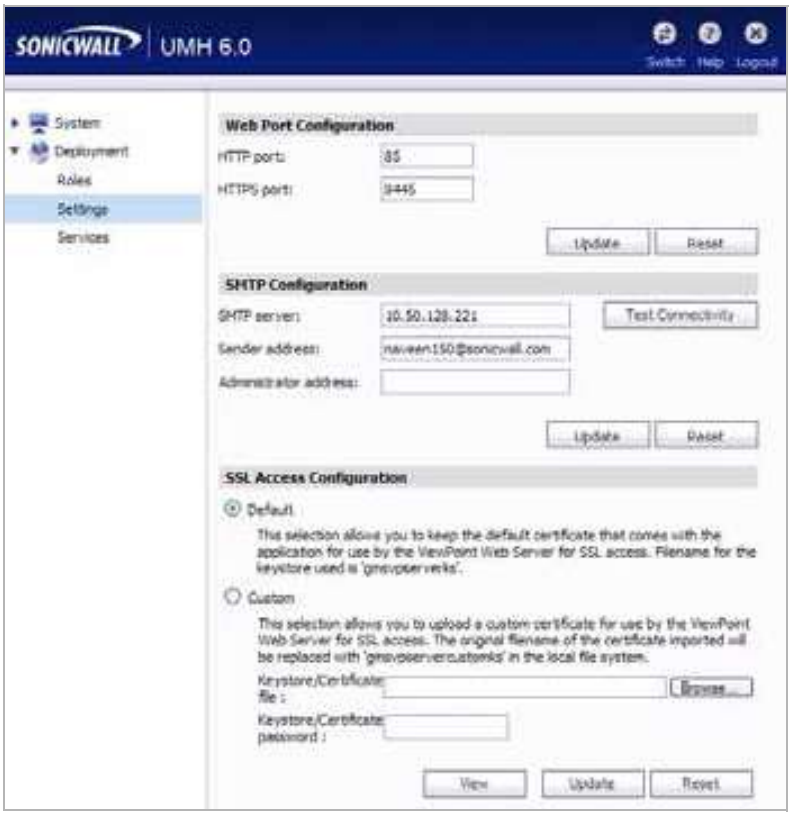


When finished, click **Update** to apply the changes. To revert the fields on the page to their default settings, click **Reset**.

Keysight, EX-1030
Page 199

Configuring Deployment Settings

The Deployment > Settings page provides a way to set the Web ports, the SMTP server IP address with the sender and administrator email addresses, and the SSL access configuration.



To configure the Web ports, enter the desired port numbers into the **HTTP Port** and **HTTPS Port** fields, and then click **Update**.

To configure the SMTP settings, perform the following steps:

1. In the **SMTP Server** field, enter the IP address or fully qualified domain name of the SMTP server. This is normally the same server that handles your regular email service.
2. In the **Sender Address** field, enter the email address, including domain, by which SonicWALL ViewPoint will be known when sending email.
3. In the **Administrator Address** field, enter the email address of the administrator who will receive email alerts and other email communications from SonicWALL ViewPoint.
4. Under SSL Access Configuration, select one of the following settings:

- **Default** – Keep the default certificate that comes with the application for use by the ViewPoint Web Server for SSL access. The filename for the keystore is **gmsvpserverks**.
- **Custom** – Upload a custom certificate for use by the ViewPoint Web Server for SSL access. The original filename of the imported certificate is replaced with **gmsvpservercustomks** in the local file system.

  Click **Browse** and select the certificate file for the **Keystore/Certificate file** field and type the password into the **Keystore/Certificate password** field.

  To display information contained in the certificate, click **View**.

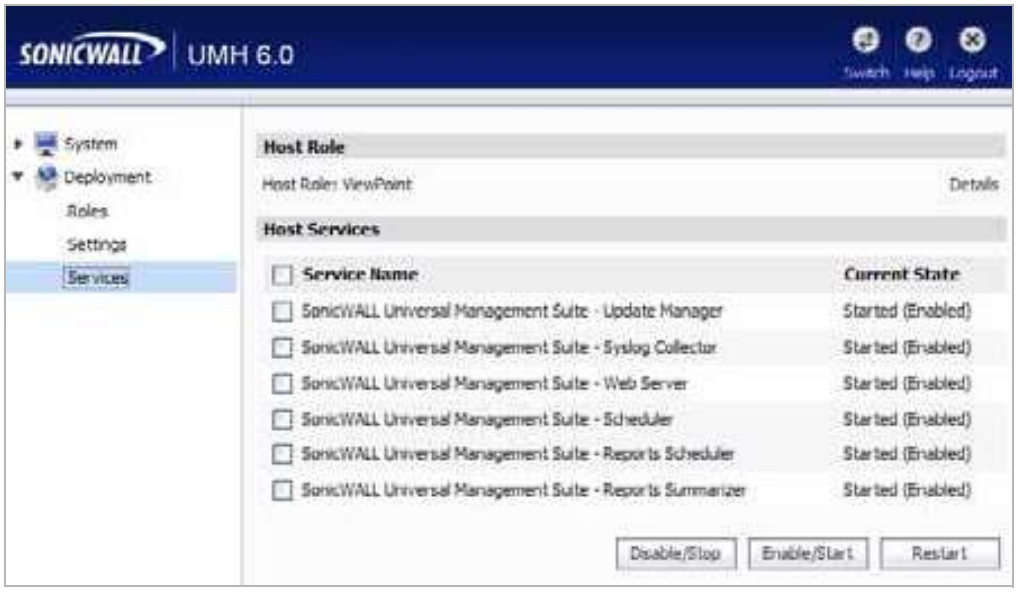


5. When finished, click **Update** to apply the changes. To revert the fields on the page to their default settings, click **Reset**.

Keysight, EX-1030
Page 201

Controlling Deployment Services

The Deployment > Services page provides a list of the services that are running on your system as part of SonicWALL ViewPoint. It also provides a way to stop or start any of the services.



To stop a service that is currently Enabled, select the checkbox for that service and then click **Disable/Stop**.

To start a service that is currently Disabled, select the checkbox for that service and then click **Enable/Start**.

To restart a service that is either Enabled or Disabled, select the checkbox for that service and then click **Restart**.

CHAPTER 3
Adding SonicWALL Appliances

This chapter describes how to add SonicWALL appliances to SonicWALL ViewPoint. . This chapter contains the following sections:

- "Adding SonicWALL Appliances to SonicWALL ViewPoint" on page 37
- "Deleting SonicWALL Appliances from ViewPoint" on page 39

Adding SonicWALL Appliances to SonicWALL ViewPoint

SonicWALL ViewPoint checks with the SonicWALL licensing server when you add an appliance, so it is important that ViewPoint has Internet access to the server.

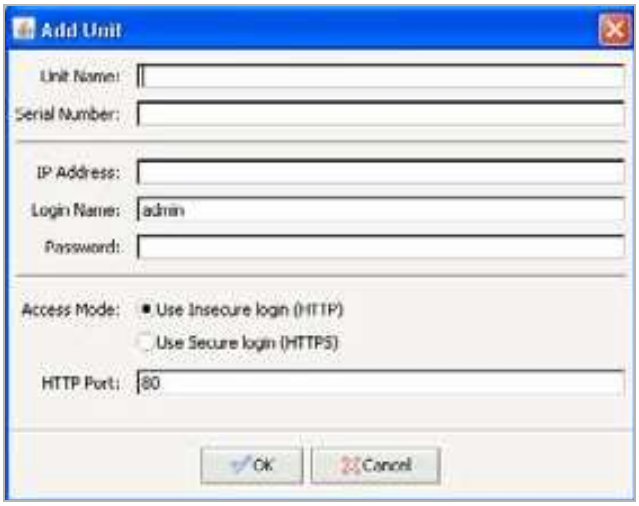
SonicWALL ViewPoint can communicate with SonicWALL appliances through HTTP or HTTPS. See the following sections:

- "Adding SonicWALL Appliances" on page 38
- "Modifying SonicWALL Appliance Settings" on page 39

Adding SonicWALL Appliances

To add a SonicWALL appliance using the SonicWALL ViewPoint management interface, follow these steps:

1. Click the appliance tab that corresponds to the type of appliance that you want to add: **UTM** or **SSL-VPN**.
2. Right-click in the left pane (TreeControl pane) of the SonicWALL ViewPoint management interface and select **Add Unit**. The Add Unit dialog box appears.



3. Enter a descriptive name for the SonicWALL appliance in the **Unit Name** field.

Note Do not enter the single quote character (‘) in the **Unit Name** field.

4. Enter the serial number of the SonicWALL appliance in the **Serial Number** field.
5. Enter the IP address of the SonicWALL appliance in the **IP Address** field.
6. Enter the administrator login name for the SonicWALL appliance in the **Login Name** field.
7. Enter the password used to access the SonicWALL appliance in the **Password** field.
8. For **Access Mode**, select from the following:
   - If the SonicWALL appliance will be connected over HTTP, select **Use Insecure login (HTTP).**

– If the SonicWALL appliance will be connected over HTTPS, select **Use Secure login (HTTPS).**

9. Enter the port used to connect to the SonicWALL appliance in the **HTTP(S) Port** field (default ports are HTTP: 80; HTTPS: 443).
10. Click **OK**. The new SonicWALL appliance appears in the SonicWALL ViewPoint management interface. It will have a yellow icon that indicates it has not yet been successfully acquired.

    SonicWALL ViewPoint will then attempt to set up an HTTP or HTTPS connection to access the appliance. ViewPoint then reads the appliance configuration and acquires the SonicWALL appliance for reporting. This will take a few minutes.

    After the SonicWALL appliance is successfully acquired, its icon turns blue, its configuration settings are displayed at the unit level, and its settings are saved to the database.

Modifying SonicWALL Appliance Settings

If you make a mistake or need to change the settings of an added SonicWALL appliance, you can manually modify its settings or how it is managed.

To modify a SonicWALL appliance, perform the following steps:

1. Right-click the appliance name in the left pane of the SonicWALL ViewPoint UI and select **Modify Unit** from the pop-up menu. The Modify Unit dialog box appears.
2. The Modify Unit dialog box contains the same options as the Add Unit dialog box. For descriptions of the fields, see Adding SonicWALL Appliances to SonicWALL ViewPoint, page 37.
3. When you have finished modifying options, click **OK**. The SonicWALL appliance settings are modified.

Deleting SonicWALL Appliances from ViewPoint

To delete a SonicWALL appliance from ViewPoint, perform the following steps:

1. Right-click on a SonicWALL appliance in the left pane and select **Delete** from the pop-up menu.

2. In the warning message that displays, click **Yes**. The SonicWALL appliance is deleted from ViewPoint.

Keysight, EX-1030
Page 206

CHAPTER 4

Using the SonicToday Panel

This chapter introduces the SonicToday panel in the SonicWALL ViewPoint management interface. .

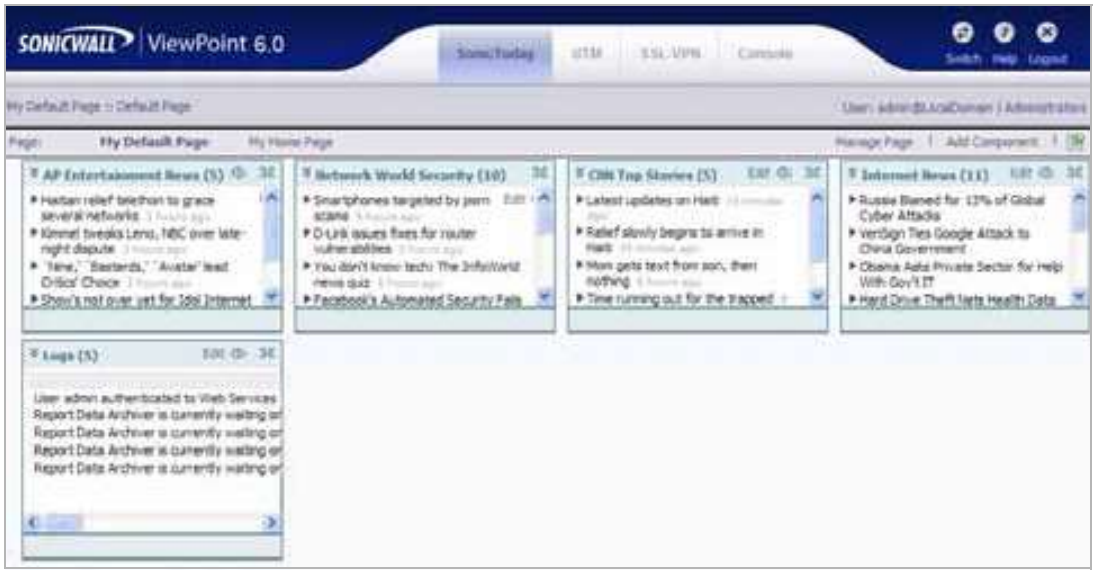
This section includes the following subsections:

- "Overview of the SonicToday Panel" section on page 42
- "Editing a Component Window" section on page 42
- "Adding a Component Window" section on page 44
- "Adding More Pages" section on page 47
- "Editing and Deleting Pages" section on page 48
- "Other Features" section on page 49

Overview of the SonicToday Panel

Using RSS and AJAX technology, SonicToday is a tab intended to work as a customizable dashboard where you are able to monitor the latest happenings with your SonicWALL ViewPoint 6.0 deployment, your network, the IT and Security World, as well as the rest of the world.

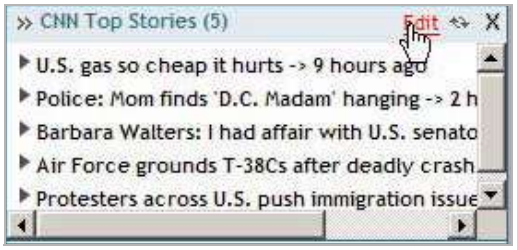
Upon initial login, you see a default **SonicToday** tab. You are able to further customize this page by configuring and adding preferred components.



Editing a Component Window

One customizable feature of SonicToday is the ability to edit the title of any given component window. To do this:

1. Click the **Edit** link, located on the right side of the component window you wish to modify. In this example, we will modify the title of the component window “CNN Top Stories.”



Keysight, EX-1030
Page 208

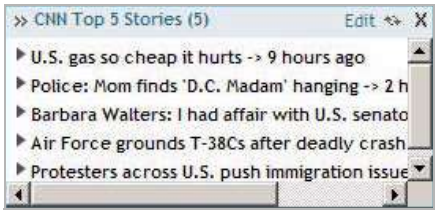
2. The component window will expand, revealing the following entries you can modify:

Title – The title of the component window.
RSS URL – The URL of the RSS Feed the current component window updates from.
Items – The number of items to be displayed on the component window.
Refresh Interval – The frequency of time the component window will refresh the RSS Feed.



In this example, we will change the title to “CNN Top 5 Stories.” For **Items**, we specify that we want five items shown in the component window, and we want the **Refresh Interval** to occur every 30 minutes. Click **Save** to save your changes and exit the component window.

The changes will update the component window immediately.



Keysight, EX-1030
Page 209

Adding a Component Window

Another way to fully customize your SonicToday dashboard is by adding a component window specifically to your preferences.

Note that no component containing the same content can be added more than once in the SonicToday dashboard.

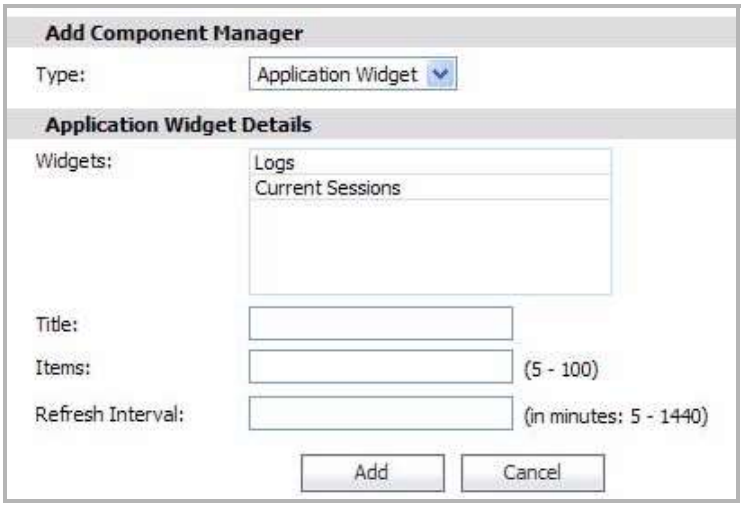
In this section, there are different component windows you can add:

- “Application Widget” section on page 44
- “RSS Feed” section on page 46

Application Widget

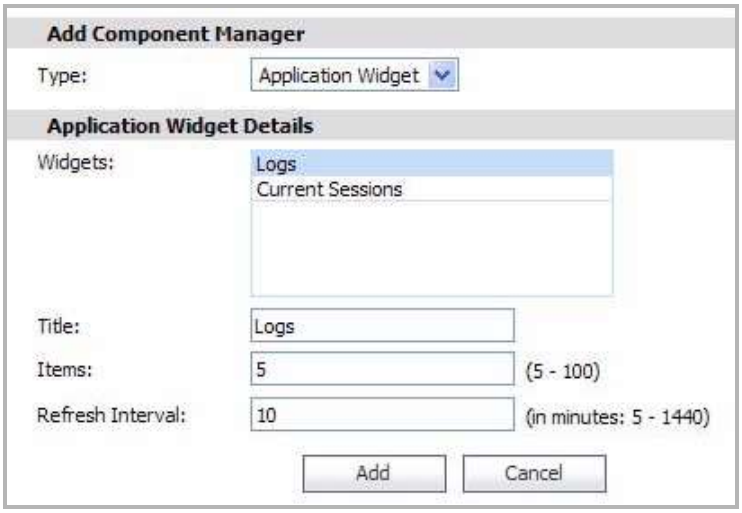
The application widget specifically details Logs and Current Sessions in SonicWALL ViewPoint 6.0. The convenience of this new widget is that it enables you to keep track of all these different details from the SonicToday dashboard page, rather than navigating through other tabs. To add the application widget:

1. Click **Add Component** to bring up the Add Component Manager dialogue box. Select **Application Widget** from the ‘Type’ drop-down list.



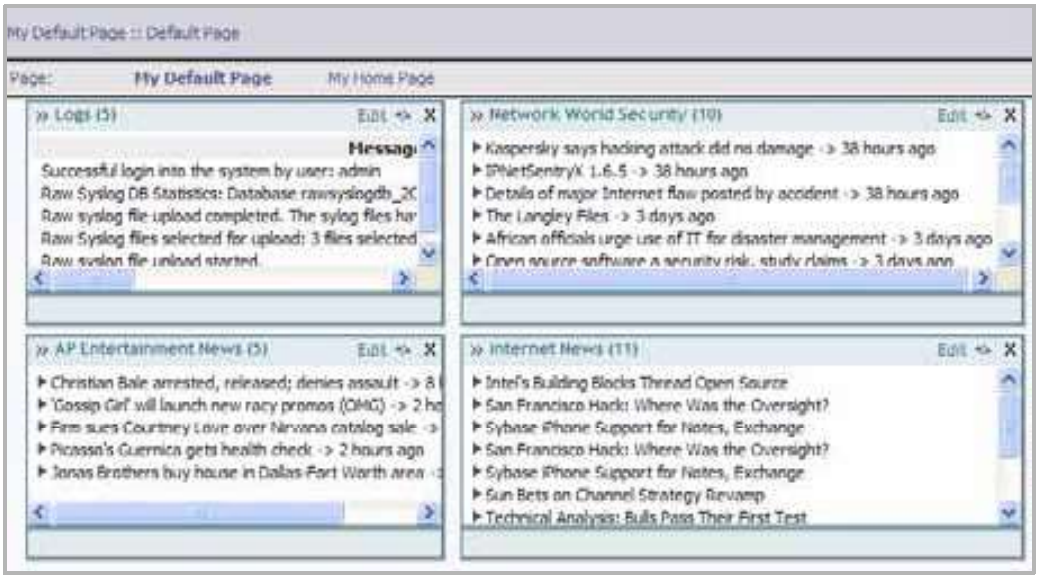
2. Specify what type of **Widget** you want in the component. The **Title** will default to the Widget you choose, but you may customize this if you prefer. You also will indicate how many **Items** you want to be shown on the component window, as well as the **Refresh Interval.**

   In this example, we will add a widget that monitors Logs, displaying the latest five everyten minutes.



3. Click **Add** when finished specifying entries. The component window is added to the SonicToday dashboard.

thanks



RSS Feed

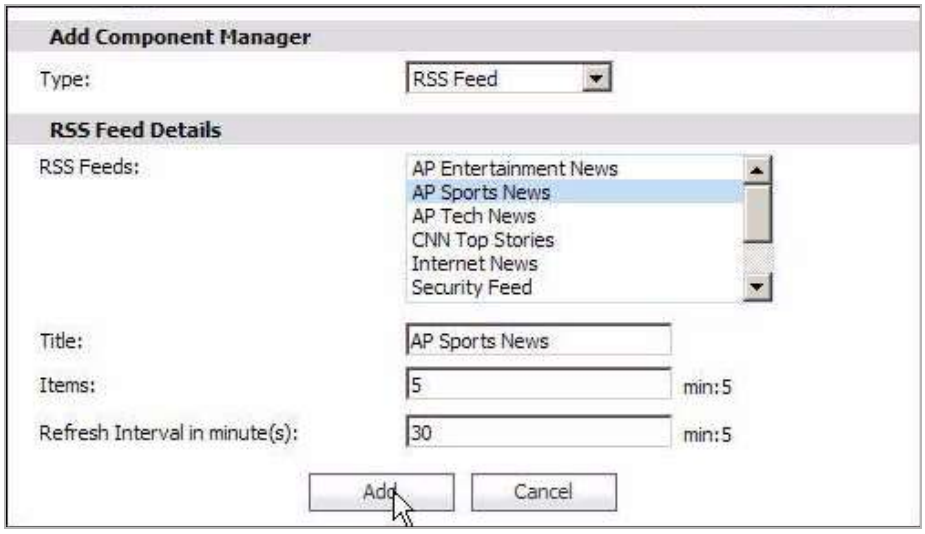
RSS Feed is a component window designed to keep you updated with what is going on in the IT and Security World, as well as all around the globe. This section contains procedures for customizing an RSS Feed component window on your SonicToday dashboard.

To choose a Predefined RSS Feed:

1. Click **Add Component** to bring up the Add Component Manager dialogue box.
2. Select **RSS Feed** from the 'Type' drop-down list. This will automatically bring up a list of predefined RSS Feeds you may choose from.

   The **Title** will default to the Alert Type you choose, but you may customize this if you prefer. You also will indicate how many **Items** you want to be shown on the component window, as well as the **Refresh Interval.**

   In this example, we will select 'AP Sports News,' displaying the first five items every 30 minutes on the component window.



3. Click **Add** when you are finished. This will add the new RSS Feed component window to your SonicToday dashboard.

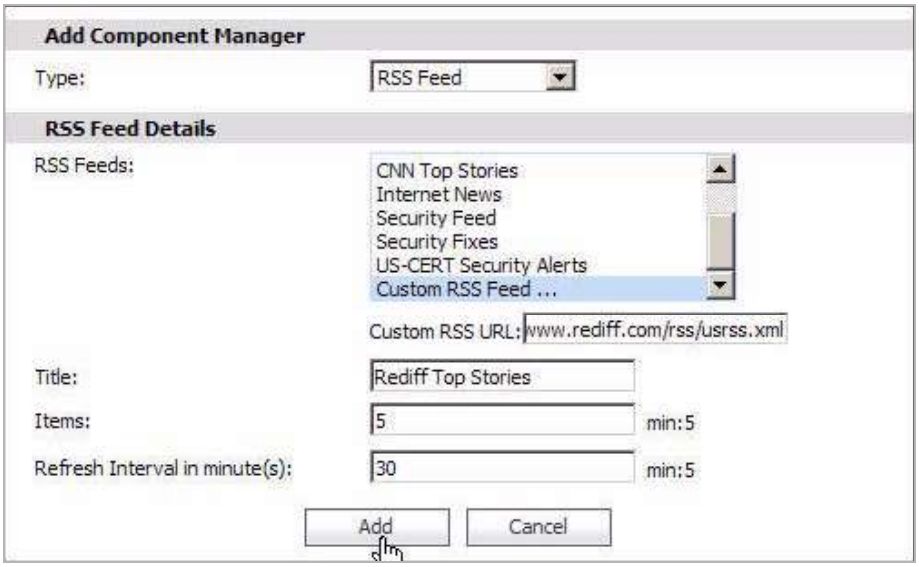
To Choose a Custom RSS Feed:

1. Click **Add Component** to bring up the Add Component Manager dialogue box.
2. Select **RSS Feed** from the 'Type' drop-down list. This will automatically bring up a list of predefined RSS Feeds you may choose from.
3. Scroll to the bottom of the predefined list and select **Custom RSS Feed...** Enter the URL of the RSS Feed you would like on your component window.

Note To search a large directory of available RSS Feeds, navigate to: http://www.rsfeeds.com/

4. Enter the **Title** for this custom RSS Feed page. Also indicate how many **Items** you want to be shown on the component window, as well as the **Refresh Interval**.

   In this example, we will choose 'Rediff Top Stories,' displaying the first five items every 30 minutes on the component window.



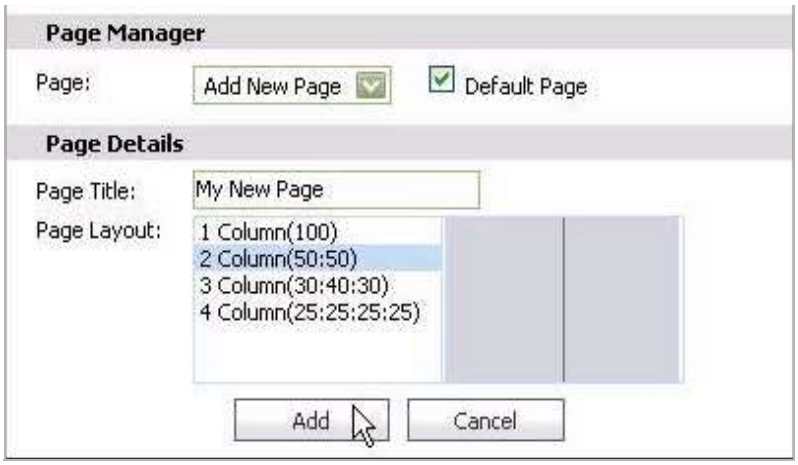
5. Click **Add** when you are finished. This will add the new RSS Feed component window to your SonicToday dashboard.

Adding More Pages

SonicToday allows you to create more pages in addition to your default dashboard page. Note that only one page may be designated as your SonicToday default page. As soon as a new page is marked as the default, any previous default page settings are overwritten. To create a new page:

1. Click **Manage Page** from the toolbar to bring up the Page Manager.
2. In the 'Page' section, select **Add New Page** from the drop-down list.
3. Name your new page under 'Page Title.'
4. Select the layout of your page under 'Page Layout.' A thumbnail image pops up alongside each option to assist you.

5. You also have the option of making this your default page, simply by placing a checkmark in the box labeled ‘Default Page.’



6. Click **Add** when you are finished. The toolbar now displays the newly added page.
In this example, we titled the new page ‘News.’



You can now add and customize component windows to navigate between pages.

Editing and Deleting Pages

To edit a page, click **Manage Page** from the toolbar. Select the page you wish to edit, make your changes, and click **Edit** to finish.

To delete a page, click **Manage Page** from the toolbar. Select the page you wish to delete and click **Delete**. Click **OK** to finish.

Other Features

See the following sections:

- AutoHide, page 49
- Page Selector, page 49
- Component Height Resize, page 50
- Manual Refresh, page 50
- Removing or Deleting a Component, page 50
- Minimizing or Maximizing a Component, page 50

AutoHide

AutoHide is a feature you customize by turning on or off. When AutoHide is turned on, the control bar will hide after an interval of two seconds when the mouse is moved away from the control bar. When AutoHide is turned off, the control bar always appears on the SonicToday dashboard.

To turn AutoHide on, click the **Off** icon  .

To turn AutoHide off, click the **On** icon 

Page Selector

Whenever the number of pages added to the SonicToday dashboard exceeds five, a page selector bar appears at the top of the main window with left and right arrows. The arrows can be used to scroll across different pages in both directions. By default, the selector is scrolled to a point where the default page appears on it. Any page can be selected by clicking on the page title.

Component Height Resize

The height of a component can be increased and decreased by stretching or shrinking the resize cursor on the status bar when the mouse is moved over the status bar.



Manual Refresh

Aside from the automatic refresh, which you configure in the "Editing a Component Window" section on page 42, you can force a refresh on the component window by clicking the **refresh** icon on the component window header.

Removing or Deleting a Component

Any component window can be removed or deleted from the page by clicking the **close** icon on the component window header.

Minimizing or Maximizing a Component

Each component can be in minimized or maximized state. The components are loaded in the page with the state they were saved in the database.

To minimize a component window, click the **minimize** icon in the component window header.

To maximize a component window, click the **maximize** icon in the component window header.

CHAPTER 5
Configuring User Settings

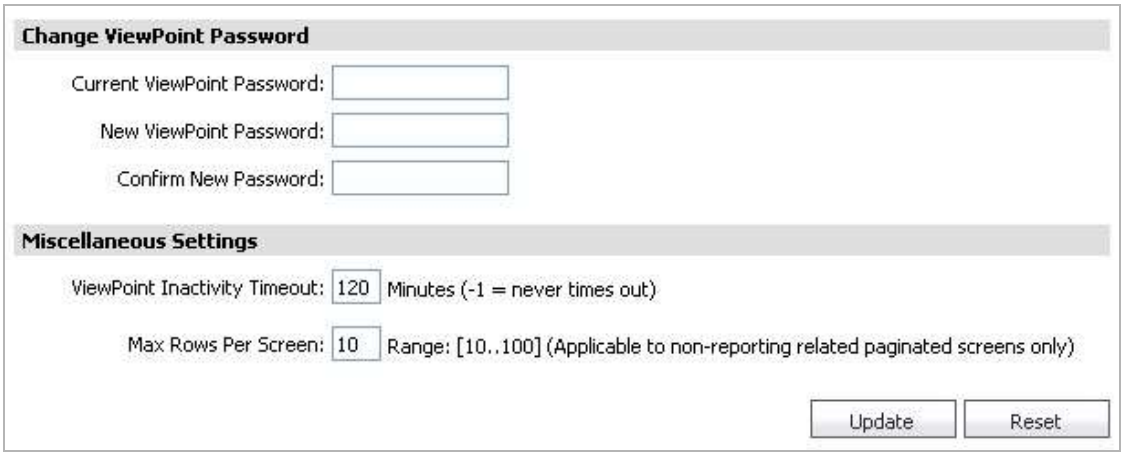
This chapter describes how to configure the user settings that are available in the Console panel on the User Settings screens.

This chapter includes the following sections:

- "Configuring General Settings" section on page 51
- "Configuring Reports Settings" section on page 53

Configuring General Settings

This section describes the **User Settings > General** page, which provides a way to change the ViewPoint administrator password, the ViewPoint inactivity Timeout, and pagination settings.



Perform the following steps:

1. Enter the existing SonicWALL ViewPoint password in the **Current ViewPoint Password** field.
2. Enter the new SonicWALL ViewPoint password in the **New ViewPoint Password** field.
3. Reenter the new password in the **Confirm New Password** field.



Note Password fields will be grayed out for users on a Remote Domain.

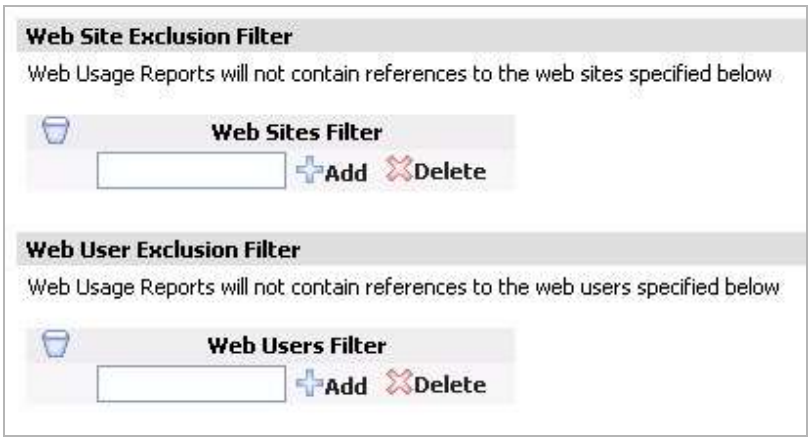
4. The ViewPoint Inactivity Timeout period specifies how long SonicWALL ViewPoint waits before logging out an inactive user. To prevent someone from accessing the SonicWALL ViewPoint UI when SonicWALL ViewPoint users are away from their desks, enter an appropriate value in the **ViewPoint Inactivity Timeout** field. You can disable automatic logout completely by entering a “-1” in this field. The minimum is 5 minutes and the maximum is 120 minutes.
5. Select a value between 10 and 100 in the **Max Rows Per Screen** field. This value applies only to non-reporting related paginated screens.
6. When you are finished, click **Update**. The settings are changed. To clear all screen settings and start over, click **Reset.**



Note The maximum size of the SonicWALL ViewPoint User ID is 24 alphanumeric characters. The password is one-way hashed and any password of any length can be hashed into a fixed 32 character long internal password.

Configuring Reports Settings

The User Settings > Reports page on the Console panel provides settings for the Web Site Exclusion Filter and Web User Exclusion Filter. Web Usage reports will not contain references to the Web sites or users specified on this page.



The following Web Usage reports are affected by the Web Site and Web User Exclusion Filters:

- Web Usage > Summary
- Web Usage > Top Sites
- Web Usage > Top Users
- Web Usage > By User
- Web Usage > By Site
- Web Usage > By Category
- Web Usage > Over Time
- Web Usage > Top Sites Over Time
- Web Usage > Top Users Over Time
- Web Usage > By User Over Time
- Web Usage > By Category Over Time

Adding Web Sites to the Filter List

When entering the Web site to exclude, type only the site name. The filter will search for the exact value provided. In the reports, only the site name is listed, without the http:// or www prefix. So for example, http://site1.sonicwall.com would not find a match in any reports because it would be listed in the reports simply as site1.sonicwall.com.

To add a Web site to the Web Sites Filter list, perform the following steps:

1. On the Console > User Settings > Reports page, type the Web site to be excluded into the **Web Sites Filter** field.

   Enter the Web site without the http:// or www prefix.

2. Click the **Add** button.

Deleting Web Sites from the Filter List

To remove a Web site from the Web Sites Filter list, perform the following steps:

1. On the Console > User Settings > Reports page, select the checkbox next to the Web site to be removed from the exclusion list. To select all sites in the list, select the **Select All** checkbox.
2. Click the **Delete** button.

Adding Web Users to the Filter List

To add a user to the Web Users Filter list, perform the following steps:

1. On the Console > User Settings > Reports page, type the user name to be excluded into the **Web Users Filter** field.

   Enter the user name without the domain.

2. Click the **Add** button.

Deleting Web Sites from the Filter List

To remove a Web user from the Web Users Filter list, perform the following steps:

1. On the Console > User Settings > Reports page, select the checkbox next to the user to be removed from the exclusion list. To select all users in the list, select the **Select All** checkbox.
2. Click the **Delete** button.

Keysight, EX-1030
Page 222

CHAPTER 6
Configuring Log Settings

This section describes how to configure Log Settings. This includes adjusting settings on deleting log messages after a certain period of time, and setting criteria for viewing logs.

This chapter includes the following sections:

- "Configuration" section on page 57
- "View Log" section on page 58

Configuration

The Log > Configuration screen provides a way to delete log messages older than a specific date.

To delete ViewPoint log messages, perform the following steps:

1. Click the **Console** tab, expand the **Log** tree, and click **Configuration**. The Configuration page displays.

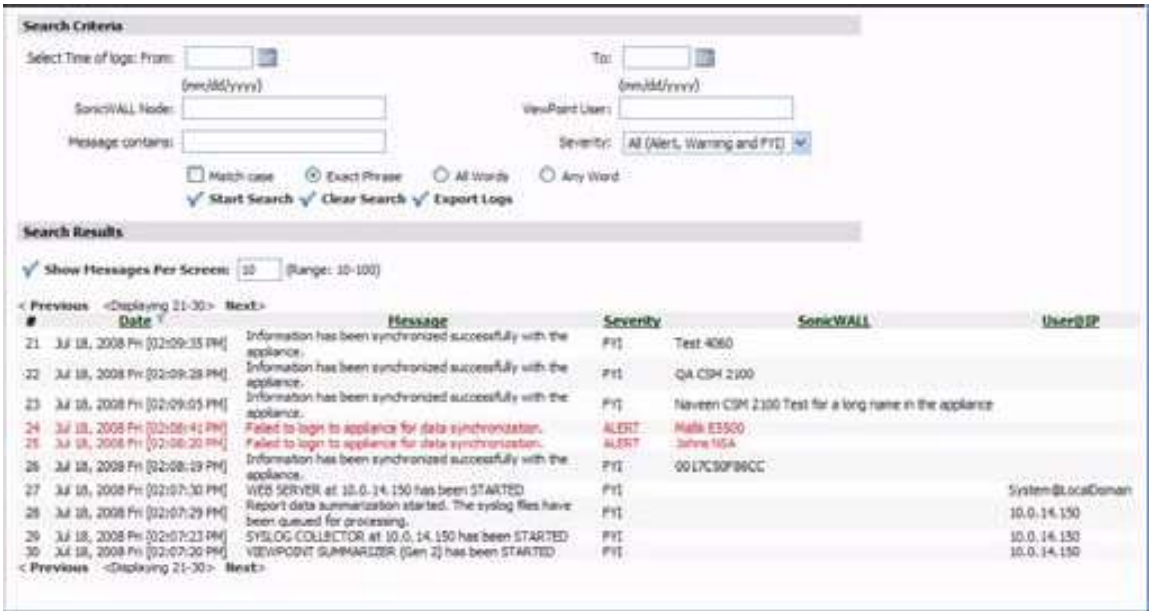


2. Select the month, day, and year from the drop down menu.
3. Click **Delete Log Messages Older Than.**

View Log

The SonicWALL ViewPoint log keeps track of changes made within the SonicWALL ViewPoint UI, logins, failed logins, logouts, password changes, scheduled tasks, failed tasks, completed tasks, raw syslog database size, syslog message uploads, and time spent summarizing syslog data. To view the SonicWALL ViewPoint log, perform the following steps:

1. Click the Console tab, expand the Log tree, and click **View Log**. The View Log page displays.



2. Each log entry contains the following fields:
   - **#**—specifies the number of the log entry.
   - **Date**—specifies the date of the log entry.
   - **Message**—contains a description of the event.
   - **Severity**—displays the severity of the event (Alert, Warning, or FYI).
   - **SonicWALL**—specifies the name of the SonicWALL appliance that generated the event (if applicable).
   - **User@IP**—specifies the user name and IP address.
3. To narrow the search, configure some of the following criteria:

Tip You can press Enter to navigate from one form element to the next in this section.

- **Select Time of logs**—displays all log entries for a specified range of dates.
- **SonicWALL Node**—displays all log entries associated with the specified SonicWALL appliance.
- **ViewPoint User**—displays all log entries with the specified user.
- **Message contains**—displays all log entries that contain the specified text. This input field provides an auto-suggest functionality that uses existing log message text to predict what you want to type. It fills in the field with the suggested text and you can either press **Tab** to accept it or keep typing. Different suggestions will appear as you continue to type if log messages match your input.
- **Severity**—displays log entries with the matching severity level:
  - All (Alert, Warning, and FYI)–where FYI mean “For Your Information”
  - Alert and Warning
  - Alert
- Select the **Match case** checkbox to make the **SonicWALL Node**, **ViewPoint User**, and **Message contains** search fields case sensitive.
- Select one of **Exact Phrase**, **All Words**, or **Any Word.**
  - **Exact Phrase** matches a log entry that contains exactly what you typed in the **Message contains** field
  - **All Words** matches a log entry that contains all the words you typed in the **Message contains** field, but the words can be non-consecutive or in any order
  - **Any Word** matches a log entry that contains any of the words you typed in the **Message contains** field

4. To view the results of your search criteria, click **Start Search**. To clear all values from the input fields and start over, click **Clear Search**. To save the results as an HTML file on your system, click **Export Logs** and follow the on-screen instructions.
5. To configure how many messages are shown per screen, enter a new value between 10 and 100 in the **Show Messages Per Screen** field. (default: 10). Click **Next** to display the next page, or click **Previous** to display the preceding page.

Keysight, EX-1030
Page 226

CHAPTER 7
Configuring Management Settings

This chapter describes the settings available on the Console panel in the Management section. The following sections are found in this chapter:

- “Settings” section on page 61
- “Alert Settings” section on page 64
- “Sessions” section on page 65
- “Database Maintenance” section on page 66

Settings

On the Console > Management >Settings page, you can configure email settings, set the system debug level, synchronize model codes information, and configure password security settings..

This section describes the following Settings topics:

- “Configuring Email Settings” on page 62
- “Configuring System Debug Level” on page 62
- “Enforcing Password Security” on page 63
- “Synchronizing Model Codes” on page 63

Configuring Email Settings

An SMTP server and an email address are required for sending ViewPoint reports.

If the Mail Server settings are not configured correctly, you will not receive important email notifications, such as:

- System alerts for your SonicWALL ViewPoint deployment performance
- Availability of product updates, hot fixes, or patches
- Scheduled Reports

To configure these email settings:

1. Click the **Console** tab.
2. Expand the **Management** tree and click **Settings**. The Settings page displays.
3. Type the IP address of the Simple Mail Transfer Protocol (SMTP) server into the **SMTP Server** field. This server can be the same one that is normally used for email in your network.
4. Type the email account name and domain that will appear in messages sent from the SonicWALL ViewPoint into the **ViewPoint Sender's e-Mail Address** field.
5. When finished in the Settings page, click **Update**. To clear the screen settings and start over, click **Reset.**

Configuring System Debug Level

SonicWALL ViewPoint provides the **System Debug level** option to control the debug messages sent to the log file.

To configure this setting:

1. Select a debug level from the **System Debug level** drop-down list. The range is 0-3 where a level of 0 provides no debug log messages and a level of 3 provides the maximum number of debug messages.
2. When finished in the Settings page, click **Update**. To clear the screen settings and start over, click **Reset.**

Enforcing Password Security

SonicWALL ViewPoint supports enforced password rotation for enhanced security compliance.

To enable and configure enforced password rotation:

1. Select the **Enforce Password Security** checkbox.
2. In the **Number of days to force password change** field, enter a value. The default is 90. SonicWALL ViewPoint will prompt the administrator to change the admin account password after the specified number of days.
3. When finished in the Settings page, click **Update**. To clear the screen settings and start over, click **Reset.**

Synchronizing Model Codes

The Sync Model Codes feature accommodates new SonicWALL product introductions without the need for ViewPoint update. When SonicWALL updates the the corporate server (MySonicWALL) with a new product code, it then becomes available to ViewPoint. The task is scheduled to run every 24 hours and is also available manually.

To synchronize model codes immediately:

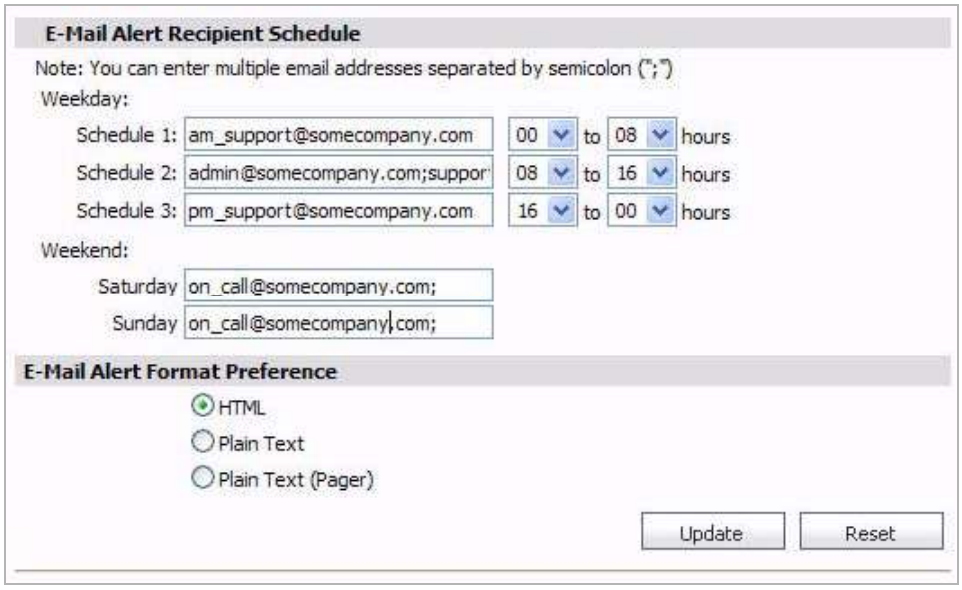
1. On the Console > Management > Settings page, click **Sync Model Codes information now.**
2. A short time later the page is updated to display the synchronization status at the top.

Alert Settings

The Alert Settings page specifies which email addresses receive email alerts and notifications during specific times.

To configure the alert notification settings, perform the following steps:

1. Click the **Console** tab, expand the **Management** tree and click **Alert Settings**. The Alert Settings page displays.



2. Configure the email address(es) that will receive notifications and the times that they will receive them:
   - **Schedule 1**—Specifies who will receive notifications during the first weekday schedule. Enter one or more email addresses (separated by commas) and specify the start and end time for the shift.
   - **Schedule 2**—Specifies who will receive notifications during the second weekday schedule. Enter one or more email addresses (separated by commas) and specify the start and end time for the shift.
   - **Schedule 3**—Specifies who will receive notifications during the third weekday schedule. Enter one or more email addresses (separated by commas) and specify the start and end time for the shift.
   - **Saturday**—Specifies who will receive notifications on Saturday. Enter one or more email addresses (separated by commas) and specify the start and end time for the shift.
   - **Sunday**—Specifies who will receive notifications on Sunday. Enter one or more email addresses (separated by commas) and specify the start and end time for the shift.

3. Select whether the email alert will be sent as **HTML**, **Plain Text**, or **Plain Text (Pager**). The Pager setting sends a very short email to ensure that the email is not cut off by the character limits of some pagers.
4. When you are finished, click **Update**. The settings are saved.

Sessions

The Sessions page of the Management section of the ViewPoint Console allows you to view session statistics for currently logged in ViewPoint users and to end selected sessions.

Managing Sessions

On occasion, it may be necessary to log off other user sessions. To do this, perform the following steps:

1. Click the **Console** tab, expand the **Management** tree and click **Sessions.** The Sessions page displays.



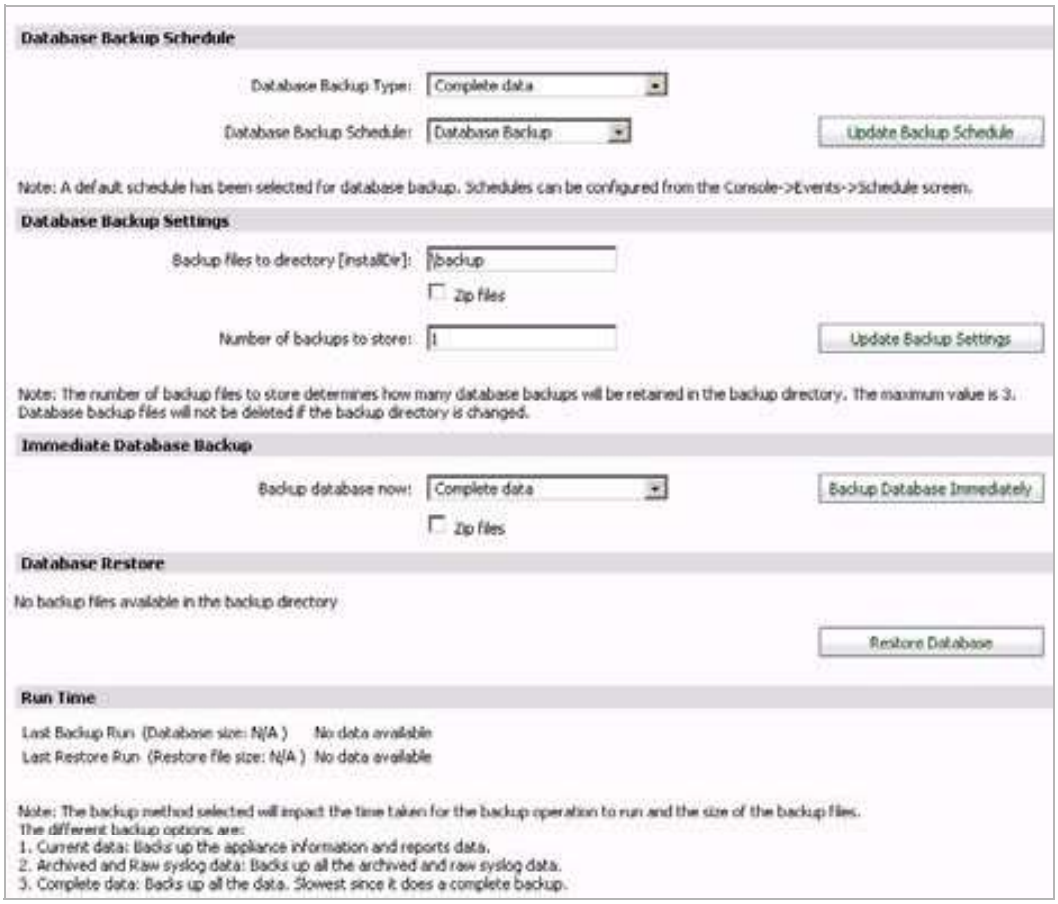
2. When more than one session is active, a checkbox is displayed next to each row. Select the check box of each user to log off and click **End selected sessions.**

   The selected users are logged off.

Database Maintenance

The Database Maintenance page allows you to back up the MySQL databases used by SonicWALL ViewPoint. This screen is not applicable to deployments using SQL Server.

Note The Console > Management > Database Maintenance page only appears in the management interface when a MySQL database is being used.



You can configure the type of backup, schedule for periodic backups, folder for backup storage, and number of backups (up to 3) to keep. You can also perform an immediate database backup from this page. Existing backups of the database are listed, and you can select from them to restore your databases.

See the following sections:

- Configuring Backup Schedule and Settings, page 67
- Backing Up a Database Immediately, page 68
- Restoring a Database Backup, page 68

Configuring Backup Schedule and Settings

To configure the database backup schedule and settings, perform the following steps:

1. Click the **Console** tab, expand the **Management** tree, and click **Database Maintenance**. The Database Maintenance page displays.
2. Under Database Backup Schedule, select one of the following from the **Database Backup Type** drop-down list:
   - **Current data** – Backs up system information and all data in **sgmsdb** for the current month; **sgmsdb** contains summarized report data
   - **Archived and Raw syslog data** – Backs up the archived data that is moved from **sgmsdb** to other files at the end of every month, and backs up raw syslog data
   - **Complete data** – Backs up all data including **sgmsdb** and all archived data and raw syslog data; this option requires the most time
3. Select the desired backup schedule from the **Database Backup Schedule** drop-down list. You can select a pre-configured schedule or a custom schedule, which you can configure in the Console > Events > Schedule screen.
4. When finished selecting options under Database Backup Schedule, click the **Update Backup Schedule** button.
5. Under Database Backup Settings in the **Backup files to directory [installDir]** field, enter the folder name in which you want to store the backup files.
6. Select the **Zip files** checkbox if you want the backup to be compressed and stored as a **.zip** file.
7. In the **Number of backups to store** field, enter the number of backups you want to store. The maximum is 3. When the maximum number of backups is reached in the configured folder, the oldest one will be removed when a new backup is created. If the folder is changed, existing backups in the previous folder will not be deleted.

8. When finished selecting options under Database Backup Settings, Select the **Zip files** checkbox if you want the backup to be compressed and stored as a **.zip** file.
9. When finished selecting options under Database Backup Settings, click the **Update Backup Settings** button.

Backing Up a Database Immediately

To perform an interactive backup of a database, complete the following steps:

1. On the Console > Management > Database Maintenance page, under **Immediate Database Backup**, select the type of backup from the **Backup database now** drop-down list. You can select one of the following types:
   - **Current data** – Backs up system information and all data in **sgmsdb** for the current month; **sgmsdb** contains summarized report data
   - **Archived and Raw syslog data** – Backs up the archived data that is moved from **sgmsdb** to other files at the end of every month, and backs up raw syslog data
   - **Complete data** – Backs up all data including **sgmsdb** and all archived data and raw syslog data; this option requires the most time
2. Select the **Zip files** checkbox if you want the backup to be compressed and stored as a **.zip** file.
3. Click the **Backup Database Immediately** button.
4. In the confirmation dialog box, click **OK.**

Restoring a Database Backup

This feature allows the administrator to restore a previously backed-up database file.



Note All services except the Web Server and the Database Service should be manually stopped before restoration is started to avoid corruption of data.

To restore your database with one of your backups, perform the following steps:

1. On the **Console > Management > Database Maintenance** page, under **Database Restore**, select the radio button for the backup that you want to restore.



2. Click the **Restore Database** button.
3. In the confirmation dialog box, click **OK.**
4. You must restart the Web Server service manually after the backup is completed.

Keysight, EX-1030
Page 236

CHAPTER 8
Managing Reports in the Console Panel

This section describes how to configure reporting settings on the Console panel. These include how often the summary information is updated, the number of days that summary information is stored, and the number of days that raw data is stored.

The following sections are included in this chapter:

- "Settings" section on page 71
- "Summarizer" section on page 73
- "Email/Archive" section on page 81
- "Scheduled Reports" section on page 82
- "Management" section on page 87

Settings

The Settings page under Reports on the Console panel provides a check box for enabling the sort option in report tables. You can also specify the number of appliances which can have Log Viewer enabled at the same time.

See the following:

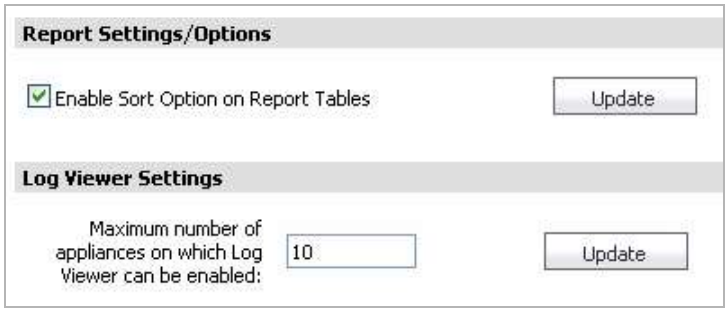
- "Enabling Report Table Sorting" section on page 72
- "Controlling the Number of Appliances with Log Viewer Enabled" section on page 72

Enabling Report Table Sorting

The Report Settings/Options section of the Console > Reports > Settings page provides a checkbox to enable the sort option on report tables.

To enable or disable the sort option for report tables, perform the following steps:

1. Click the **Console** tab, expand the **Reports** tree and click **Settings.**



2. To enable the report table sort option, select the **Enable Sort Option on Report Tables** checkbox. To disable sorting, clear the checkbox.
3. Click **Update.**

Controlling the Number of Appliances with Log Viewer Enabled

You can control the maximum number of managed appliances for which Log Viewer can be enabled. The default setting allows Log Viewer to be enabled on up to five appliances. Because enabling Log Viewer causes raw syslog data uploading, it is resource intensive. Use care in increasing this number, and when enabling Log Viewer on systems.

Log Viewer must be enabled on an appliance in order to use Custom Reports. Custom Reports are available for UTM and SSL-VPN appliances. For more information about Custom Reports, see the following:

- “Using Custom Reports on UTM Appliances” section on page 163

To change the number of appliances for which Log Viewer can be enabled:

1. On the **Console** panel, navigate to **Reports > Settings.**
2. Under **Log Viewer Settings**, in the **Maximum number of appliances on which Log Viewer can be enabled** field, enter the number of appliances for which Log Viewer can be enabled. The default is five.
3. Click **Update.**