Release Notes

Secure Remote Access | **SonicWALL Aventail E-Class SRA EX-Series 10.5.3**

Platform Compatibility

The SonicWALL Aventail E-Class SRA EX-Series 10.5.3 release is supported on the following SonicWALL appliances:

- SonicWALL Aventail E-Class SRA EX7000
- SonicWALL Aventail E-Class SRA EX6000
- SonicWALL Aventail E-Class SRA EX-2500
- SonicWALL Aventail E-Class SRA EX-1600
- SonicWALL Aventail E-Class SRA EX-750

On 64-bit Windows Vista and Windows 7 systems, this release has been tested on and supports 32-bit Internet Explorer 7 and 8.

On Windows 7 SP1 (32-bit and 64-bit), this release has been tested on and supports Internet Explorer 8 (32-bit).

On Mac OS X 10.6.4 (32-bit and 64-bit), this release has been tested on and supports Safari 5.0.x.

Note: The Java plugin sometimes fails when using Firefox 4.0 beta versions on client machines while attempting to log in to WorkPlace.

Upgrading from Earlier Versions

If you are upgrading a SonicWALL Aventail E-Class SRA EX-Series appliance to version 10.5.3 from an earlier release, be sure to consult the upgrade instructions in the *SonicWALL Aventail Upgrade Guide* for detailed information. You'll find a copy of this document on the MySonicWALL Web site (www.mysonicwall.com).

Release Caveats

The 10.5.X release series will be the last release with support for OnDemand Dynamic Mode, which is a proxy based agent deployed through the WorkPlace portal. It is important to note that the OnDemand Proxy Agent has two configurations: Dynamic Mode and Mapped Mode. **The Mapped Mode use case is still supported, and only Dynamic Mode support is being removed**.

We recommend customers who still have OnDemand Dynamic mode configured through the WorkPlace portal consider the OnDemand Tunnel agent as an alternative. The **OnDemand Tunnel agent** offers superior performance and platform coverage over OnDemand Dynamic mode, while requiring identical installation requirements.

What's New in This Release?

This version of the Aventail SonicWALL E-Class SRA EX-Series software includes the following new and enhanced features:

- **Virtualization –** The SonicWALL Aventail Virtual Appliance is supported starting with firmware version 10.5.3. Virtualization provides administrators with the ability to consolidate multiple virtual appliances onto a single physical server or a server cluster. Additionally, virtualization enables organizations to allocate additional computing resources to the virtual machine cluster as required. The SonicWALL Aventail Virtual Appliance is a software appliance that can easily be installed and configured in VMware environments.

- **Virtual Assist –** Provides administrators and helpdesk technicians with the capability to assist remote employees and users with technical assistance issues. Technicians are able to control a user's desktop and system at a distance, which provides an efficient and economical method to provide targeted technical support. Users can also request Virtual Assist sessions through the WorkPlace portal.
- **Web Policy and SSO Tunnel Support –** This tunnel URL filtering feature enforces URL-based rules within VPN tunnel sessions. This feature not only provides more effective security, but also allows the use of Single Sign-On (SSO) for Web applications accessed via a tunnel.
- **iPhone, iPad, Android and Symbian Support – ActiveSync for Exchange –** Extends SonicWALL's clientless ActiveSync support for Exchange email to mobile devices that are becoming popular choices for corporate mail. This feature also leverages the device's ID capability to link the device to a single user, providing a first layer of end-point control.
- **Aventail Connect for Android –** Aventail Connect for Android provides secure network access to client/server applications that are available for Android devices. The Aventail Connect Android client provides application layer proxy redirection similar to OnDemand Mapped mode.

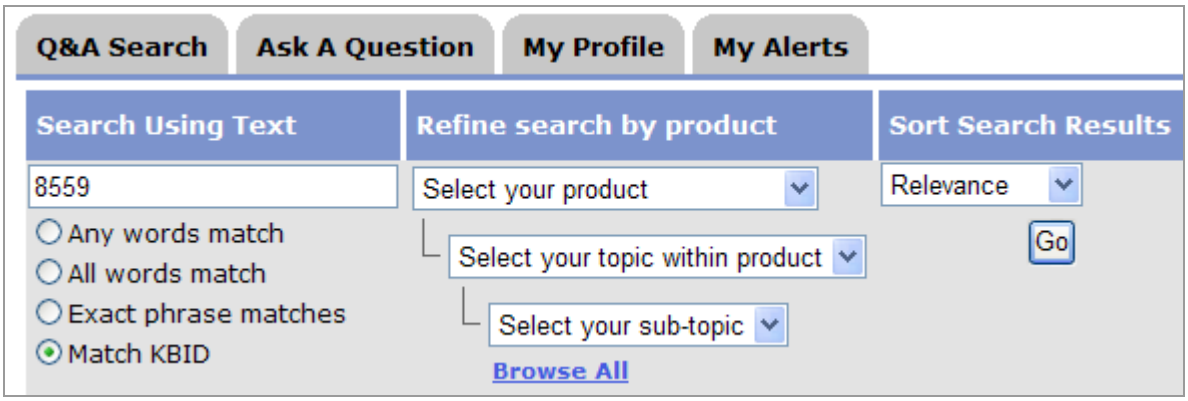
  The Android client supports creation of multiple VPN profiles, import of client certificates, all available authentication methods and basic End Point Control (EPC). After successful authentication, the client will attempt to load and start any pre-defined port-mappings specified by the admin. The end-user can also define the mappings (access is still based on policy evaluation at the appliance). Typical uses are for RDP, VNC, or SSH access to backend servers protected by the SonicWALL Aventail appliance in the company's network.

  This version is a technology preview designed to get feedback from early adopter users of Android devices with the SRA EX Series firmware. As such, Aventail Connect for Android is subject to significant change prior to its general release.

  The Aventail Connect Android client can be downloaded and installed from the Android Market free of charge.

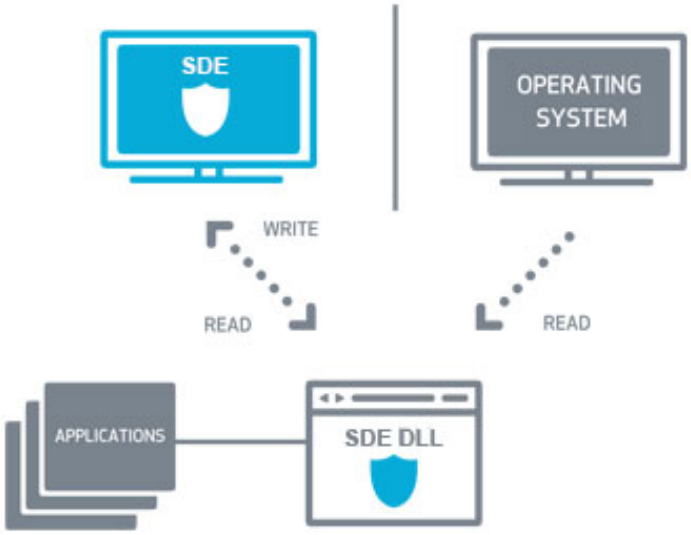
  For detailed information about installing and using the Aventail Connect Android client, refer to the latest version of the *SonicWALL Aventail 10.5 Installation and Administration Guide*, available on MySonicWALL or www.sonicwall.com.

  This information is also available in Knowledge Base article #8559, available at: http://www.sonicwall.com/us/support/kb.asp



- **Password Management for Sun and Novell Directory Servers –** Provides support to Novell and Sun LDAP servers for improved password management. This new feature calls upon the Policy server to probe and predetermine the directory server and the applicable version. End users will be able to enter LDAP credentials and be notified through the appliance when their password needs to be changed due to expiration or backend policies, and will then allow users to change the password. The following server versions are supported:
    - Sun Java System Directory Server Enterprise Edition (DSEE) 7.0
    - Novell eDirectory 8.8 SP5
- **Extension Configurations in Management UI –** A new page has been added to the Maintenance section of the AMC management interface to allow simple configurations to be completed for extensions. This new feature assists administrators in making configuration adjustments that appear in maintenance releases or hotfixes, and allows for the configuration of arbitrary key-value pairs.
- **Cache Cleaner (also known as OPSWAT CC) –** Provides VPN administrators with an end-point data protection tool to ensure data downloaded or accessed during a session is functionally wiped from the user's system. This feature removes Web browser information, such as cookies, browsing history, and stored passwords upon termination of the session. The Cache Cleaner (OPSWAT) is supported on the following platforms:
    - Windows XP SP3 or later
    - Windows Vista SP2 or later (32-bit, 64-bit)
    - Windows 7 (32-bit, 64-bit)
    - Windows 7 SP1 (32-bit, 64-bit)
    - Windows 2008 Server
    - Mac OS X 10.5 (Leopard)
    - Mac OS X 10.6 (Snow Leopard) (32-bit, 64-bit)
- **OPSWAT's Secure Desktop Emulator SDK (SDE) –** is a solution that protects people when accessing corporate applications, networks or data from unprotected devices such as home computers, public kiosks and guest laptops. A working demo of the technology is available at http://www.securevirtualdesktop.com. The accessibility of web-based applications has changed the way employees and business partners access and utilize sensitive information. On remote systems, corporate security departments cannot ensure the integrity of endpoints or prevent the compromise of enterprise assets such as company financials, customer information, and intellectual property. OPSWAT's Secure Desktop Emulator SDK is able to extend the corporate security policy by creating a fully sandboxed environment. This secure workspace, existing inside an isolated clone of the file system, ensures the security of the computer, protects the information provided by the web application, erases the information at session termination and protects the session from malware.

  How does OPSWAT's Secure Desktop Emulator work?
    - SDE is a virtual clone that sits between your applications and your hardware (hard drives, registry, copy/paste buffers, external media, printers, etc.). As applications try to read or write to these sensitive areas, SDE applies security policies from a configuration file, providing control over user access to system resources and over authorization of data sharing to and from the sandboxed environment.



The key benefits for OPSWAT's Secure Desktop Emulator:

- Enables the secure deployment of web based applications
- Protects customer, employee and corporate data accessed by unmanaged devices

SDE is ideal for any situation where security concerns dictate the need for a shadow desktop. Use SDE to:

- Increase security for users accessing important resources via SSL VPN.
- Increase security for users at WiFi hotspots, business centers, airport kiosks, conference centers, hotels, cafés, etc.
- Ensure that users are protected when you host a website that contains sensitive data (banking, accounting, etc.).
- Incorporate DLP solution features into your product.

SDE has many configuration options, allowing the following controls:

- Whitelist/blacklist specific applications
- Isolate the copy and paste buffer to exist only within the virtual environment
- Limit access to network drives on the endpoint
- Limit access to external media (USB, DVD, etc.) on the endpoint
- Control which processes are launched at startup
- Control printer access

Features of the OPSWAT's Secure Desktop Emulator:

- Simple CLI
- Small footprint
- Able to use a configuration file located on the local computer or on a server
- Preserve or delete resources upon exit
- Customize session desktop image and/or background color
- Auto termination after a specified period of inactivity
- Messaging can be localized to user environment

Currently Supported Platforms:

- Windows XP SP3 (x86, x64)
- Windows Vista RTM/SP1 (x86, x64)
- Windows 7 RTM (x86, x64)
- English language versions only

Currently Supported Browsers:

- Internet Explorer 7, 8 and 9
- Firefox 3.5+ and 3.6+
- Safari 5.3
- Google Chrome 8.0 and 9.0

Known Issues

This section describes known issues for this release. The issues are organized into the following categories:

AMC Configuration

Symptom	Condition / Workaround	Issue
Cache Cleaner performs cleanup and exits within 2 minutes after being started by a user login to WorkPlace. Cleanup and exit are shown in the tooltip and in Task Manager.	Occurs when enabling Cache Cleaner (CC) with End Inactive User Connections set to the 'Never' option on the Configure Data Protection page. The Secure Desktop Emulator works fine when End Inactive User Connections are set to the 'Never' option.	98162
AMC displays no results for searches resulting in a large number of matches.	Occurs when a search for users or groups on an external directory that results in more than 1,000 matches (on a Windows 2000 server) or 1,500 matches (on a Windows 2003 server).	61955

Cache Cleaner (OPSWAT CC)

Symptom	Condition / Workaround	Issue
Cache Cleaner clears all items including non-session history, passwords, and form data from cache history against policy.	Occurs when users are connecting through an Internet Explorer 8 or Firefox browser, even when Protected Mode is turned off in IE and when the "Clear session items only" policy option is enabled in AMC.	94097, 88556
Cache Cleaner clears all items from cache history against session-only policy.	Occurs when users on a system with Cache Cleaner enabled close out of a browsing session. Cache Cleaner clears all items from the cache, even when clearing scope is set to "Clear session items only" in AMC. Occurs on a Mac OS X 10.6.3 client system with Safari or on a Windows XP SP3 client system with Internet Explorer 8 and Protected Mode turned off.	90104, 89001

Symptom	Condition / Workaround	Issue
Cache Cleaner causes Internet Explorer to close and then reopen a tab, resulting in a warning saying “This tab has been recovered.”	Occurs when clicking Logout in WorkPlace with Cache Cleaner running, while using Windows 7 or Vista SP2 with an Internet Explorer 8 browser with Protected Mode turned on. **Workaround**: Turn Protected Mode off.	89956
Cache Cleaner does not clear the browser cache history despite a clear all items policy.	Occurs when users log in to WorkPlace with Cache Cleaner enabled, use the browser to access various Web sites, then log out of WorkPlace and close the browser, and then launch the browser again after Cache Cleaner exits. Cache Cleaner does not clear all items from the cache, although the clearing scope is set to "Clear all items" in AMC. Occurs on a 64 bit Windows Vista SP2 client system with Internet Explorer 8 and Protected Mode turned on. **Workaround**: Turn Protected Mode off in IE.	88507
The tray icon for Cache Cleaner is not displayed on the client system.	Occurs on 32-bit and 64-bit Window 7 and Vista SP2 client systems when using Internet Explorer with Protected Mode turned on. **Workaround**: Turn Protected Mode off in IE.	88453
Cache Cleaner is slow to release memory and exit after user logout.	Occurs when using Internet Explorer 8 or a Firefox browser on a Windows XP SP3 client system. A delay of 53 seconds has been observed.	88364

Certificates

Symptom	Condition / Workaround	Issue
For certain customers using Firefox 4.0 and Certificate Authentication, end-users may fail to authenticate with a Mozilla error 'ssl_error_renegotiation_not_allowed'.	Occurs due to a behavioral change by Mozilla in Firefox 4.0 and newer, requiring support for RFC 5746. **Workaround**: Include the appliance hostname(s) in the 'security.ssl.renego_unrestricted_hosts' configuration parameter. This allows certificate authentication to succeed, and does not pose any additional risk to the end-user, administrator, or appliance. SonicWALL does not support renegotiation in general in the 10.0.X and 10.5.X firmware line, and as such is not vulnerable to CVE-2009-3555.	97120

Cache Cleaner Comparison

This table lists differences in behavior between the OPSWAT Cache Cleaner and the Symantec Cache Cleaner that was included in previous releases.

#	Features	Symantec (Sygate) Cache Cleaner	OPSWAT Cache Cleaner
1	Supported platforms	Windows XP SP2 (32 bit) Windows 2000, 2003 Macintosh 10.3.9 and 10.4.9	Windows XP SP3 (32 bit) Vista SP2 (32/64) Windows7 (32/64) Windows 2003, 2008 (32/64) Macintosh 10.x
2	Supported browsers	Internet Explorer (IE) 6 and 7 Firefox (FF) 1.5 and 2.0 Safari 1.2 and 2.0 (Mac)	Internet Explorer 6, 7 and 8 FF 2, 3.0 and 3.5 Safari 3.0 and 4.0 (Mac)
3	Clearing Browser data Form data Download history	 Yes Yes	 No Not supported in Safari (Mac)
4	Support Session scope	Yes	Yes (Mostly) Instead of clearing session specific typed-URLs and cookies, all of the typed-URLs and cookies are wiped.
5	Close all browser windows at startup	Yes	No. This feature has been removed. Instead, when the user chooses to logout from WorkPlace, a prompt states all browser windows will close.
6	Post -timeout interval	The client closes browsers and then initiates a complete wipe and terminates.	The client initiates a wipe but continues to run until the browser windows are closed explicitly.
7	Wipe scope	Data in the context of the provisioning browser is wiped. For example: If the Cache Cleaner is loaded within Internet Explorer (IE), then at the end, CC only wipes data specific to IE. However, data in another supported browser (Firefox) is unmodified.	OPSWAT provides system-wide DPA. OPSWAT monitors and wipes data in all supported browsers (Internet Explorer and Firefox) and not necessarily that of provisioning-browser.

OPSWAT Cache Cleaner Deployment Issues

The following tables contain known issues and deployment results provided by OPSWAT for the Cache Cleaner when using Internet Explorer in certain environments.

Key to colors and abbreviations:

IE	Internet Explorer
PM	Protected Mode
JRE	Java Runtime Environment
RED	Failed to wipe
GREEN	Successful wipe

Launching via Applet

The following table outlines the issues that the Cache Cleaner will encounter based on different environments:

	JRE < JRE 6, update 10		**JRE >= JRE 6, update 10**	
	PM ON data	PM OFF data	PM ON data	PM OFF data
IE 7 PM ON	Cache Cookies History Typed Addresses Passwords	Cache Cookies History Typed Addresses Passwords	Cache Cookies History Typed Addresses Passwords	Cache Cookies History Typed Addresses Passwords
IE 7 PM OFF	Cache Cookies History Typed Addresses Passwords	Cache Cookies History Typed Addresses Passwords	Cache Cookies History Typed Addresses Passwords	Cache Cookies History Typed Addresses Passwords
IE 8 PM ON	Cache Cookies History Typed Addresses Passwords	Cache Cookies History Typed Addresses Passwords	Cache Cookies History Typed Addresses Passwords	Cache Cookies History Typed Addresses Passwords
IE 8 PM OFF	Cache Cookies History Typed Addresses Passwords	Cache Cookies History Typed Addresses Passwords	Cache Cookies History Typed Addresses Passwords	Cache Cookies History Typed Addresses Passwords

Launching via ActiveX

The following table outlines the issues that the Cache Cleaner will encounter based on different environment setups on Windows Vista:

	PM ON data	PM OFF data
IE 7 PM ON	Cache Cookies History Typed Addresses Passwords	Cache Cookies History Typed Addresses Passwords
IE7 PM OFF	Cache Cookies History Typed Addresses Passwords	Cache Cookies History Typed Addresses Passwords
IE8 PM ON	Cache Cookies History Typed Addresses Passwords	Cache Cookies History Typed Addresses Passwords
IE8 PM OFF	Cache Cookies History Typed Addresses Passwords	Cache Cookies History Typed Addresses Passwords

Connect Mobile

Symptom	Condition / Workaround	Issue
Installing or uninstalling Connect Mobile on a hand held device can fail.	Occurs when Trend Micro Mobile Security real-time scanning and virus detection is enabled on the device. **Workaround**: Disable real-time scanning before installing or uninstalling Connect Mobile.	60183

Connect Tunnel

Symptom	Condition / Workaround	Issue
The client may experience the error message “A server operation has exceeded its timeout value” during an attempt to reconnect using Connect Tunnel, but the second attempt works fine.	Occurs when connecting to the appliance using Connect Tunnel from a Windows 7 computer with no service pack upgrades, after the computer has been in a suspended state. This only happens when Encapsulated Security Payload is enabled because it’s timed out by EVPN.	96988
While URL Filtering is enabled, an illegal, rejected HTTP stream lets certain DENY rules fail open, allowing the rule to be circumvented and content retrieved from the back-end server.	Occurs when URL Filtering is enabled, a DENY rule exists for a specific URL resource, and an HTTP request is sent using an illegal HTTP construct that is rejected by the SonicWALL Aventail HTTP scanner, but is supported by a Web server. **Workaround**: Craft policy in accordance with best practices, using ALLOW rules to grant access to specific resources followed by a broad DENY rule disallowing access to all others. **Note**: Check the Knowledge Portal (on MySonicWALL under Support) for current hotfixes that resolve specific instances of this issue, and apply them before enabling URL Filtering.	94535
Proxy configuration on a private network leads to long Connect Tunnel connection times on some public networks.	Occurs when a private network uses a proxy for its LAN systems. When Connect Tunnel is used on public networks, it attempts to use that private LAN proxy. The problem is that an increasing number of ISP's are resolving names that have no resolution to a default site (usually advertising related). When the unresolved name does falsely resolve to an IP address, the client then attempts to load the PAC file from the resolved address. Of course, none is forthcoming, so a long timeout ensues on every new Connect Tunnel connection.	94424
On Mac OS clients, Connect Tunnel fails to determine outbound proxy settings when it is already launched.	Occurs because, on Mac clients, the System proxy configuration information is detected only when Connect Tunnel is started. If the proxy information is modified when Connect Tunnel is already running, the changes will not be reflected, and Connect Tunnel will not prompt for authentication and will not establish the connection. **Workaround**: Close and re-launch Connect Tunnel after modifying proxy information.	84422

Symptom	Condition / Workaround	Issue
Connect Tunnel fails without an error message when connecting to the 32-bit Connect Tunnel client on a 64-bit machine.	Occurs when the 32-bit Connect Tunnel client is installed on a system running Mac OS X Snow Leopard (v10.6) and the system is rebooted in 64-bit mode. **Workaround**: Upgrade earlier versions of the client to the current version of the universal (64-bit and 32-bit) Connect Tunnel client for Mac OS X 10.6 and later on machines running 64-bit Mac OS X Snow Leopard.	83801
A misleading error message is displayed: “VPN Connection Failed. Access denied. The required system capabilities are not present, enabled, or current.”	Occurs when logins are attempted after the number of users logging in to the appliance reaches the licensed limit. At issue is the license count on the appliance, not the system capabilities of the client device.	77107
Local resources are sometimes directed through an internal proxy server.	Occurs when traffic to local networks is redirected through a remote proxy with "Redirect All Non Local Mode", and can be observed by users when Connect Tunnel is enabled and the users are logged into the appliance.	63247
Tunnel clients are unable to reconnect over an access point that requires authentication.	Occurs on a Macintosh device when you switch to a network that requires authentication. For example, if a user is connected to the appliance using a wired connection and changes to a wireless access point that requires authentication, the previous connection cannot be re-established; the user must manually log in to the appliance.	61730
In Redirect All mode, the Internet is accessible if proxy settings are configured on browsers.	Occurs on both Internet Explorer (IE) and Firefox (FF) browsers when a user configures proxy settings.	61605
The desktop icon for Connect Tunnel in WorkPlace is not present for all Linux users.	Occurs when you provision Connect Tunnel from WorkPlace and the user downloads and installs the client, which normally creates an icon on the users desktop. If the client device is a computer running a Linux operating system and a different person logs in to it, no desktop icon for Connect Tunnel will be visible. **Workaround**: One workaround is to bring up the command window (press ALT+F2), and then type the path to the Connect Tunnel program. Alternatively, you could create an icon on the desktop for the Connect Tunnel program. In Redhat or Fedora, for example, you would right-click on the desktop and select Create Launcher, and then browse to the Connect Tunnel application.	61167

Symptom	Condition / Workaround	Issue
When using dial-up and remote proxy for the connection to the Internet, Internet browsing might not traverse the remote proxy.	Occurs when you use a dial-up connection to the Internet, and the community to which you are assigned is configured for remote proxy. This applies regardless of whether the remote proxy was configured manually or using a .pac file. **Workaround**: In Connect Tunnel, make sure the dial-up connection is specified on the Properties page. Select the 'Establish this connection first' check box and specify a connection in the drop-down list. (If you use OnDemand tunnel, there is no equivalent way to specify the connection properties.)	61056
Cannot access the appliance if specified proxy server is unavailable.	Occurs when Internet Explorer is configured to use an outbound HTTP proxy server and Connect Tunnel attempts to access the appliance using that proxy server. If the proxy is available, the client connection will succeed. However, if the proxy server is unavailable, the client will not fall back to sending traffic through the default route, causing the connection to the appliance to fail. **Workaround**: Remove the proxy setting from the browser.	60912
Cannot access the appliance using the FQDN/VIP for a WorkPlace site. The Connect tunnel client displays the message, "The device is not in a valid state to perform this request."	Occurs when the Connect tunnel client is configured (by an administrator or user) to access the appliance using the FQDN or virtual IP address for a custom WorkPlace site. **Workaround**: Configure the client to access the appliance using the FQDN or IP address contained in the appliance's main certificate.	59902

End Point Control

Symptom	Condition / Workaround	Issue
Smartphone ActiveSync users are classified to the default or quarantine zone even when the smartphone device ID or serial number is configured as a user attribute in the Active Directory server.	Occurs when the device ID in the user attribute does not include the specific prefix such as “Appl” or “droid” that is sent in the POST message when the smartphone connects to the appliance. **Workaround**: View the POST message in the appliance log, and use the device ID value shown there for the AD user attribute.	93443
An incorrect MS VC++ run-time error may be displayed by Internet Explorer.	Occurs when a user logs out of WorkPlace within an Internet Explorer browser when the Cache Cleaner was enabled, and then successfully removes the Cache Cleaner Control Class plug-in.	88563
Upgrading to 10.5.x from 10.0.x and previous versions with SODP enabled will fail.	Occurs because Symantec OnDemand Protection is not supported in versions 10.5.x. **Workaround**: Before upgrading to 10.5.x from 10.0.x and earlier versions, disable Symantec OnDemand Protection for all End Point Control Zones.	88186

Symptom	Condition / Workaround	Issue
Zone classification can fail in certain cases, preventing the user from logging in.	Occurs when the equipment ID was typed using lower case letters when creating the device profile, and then the user attempts to login from a machine whose equipment ID matches the ID in the device profile except that it contains upper case letters. **Workaround**: Use capital letters when entering the equipment ID into the device profile.	82465
Zone classification fails when a device profile combines values and the “Match profile if user has no registered devices” check box is selected.	Occurs when a device profile contains a combination of a hard coded equipment ID and user attributes, and the user logs in using an unregistered device. When selected, the “Match profile if user has no registered devices” check box is applicable when the user has no devices registered in the back end AD or LDAP server and there are no hard coded devices in the device profile.	81851
Zone classification fails with certificate device profile on Linux and Mac machines. The client is relegated to the default zone rather than the intended zone.	Occurs when a root certificate is imported to the appliance and configured as a device profile for either the Mac OS or Linux platform, then the zone is created including the device profile with persistent EPC enabled, and the zone is added to a realm. The client certificate is imported to the client Firefox browser and the user authenticates to the realm, but is classified to the default zone. The zone classification fails because the appliance is not integrated with the certificate store for the operating system or the browser.	69625
Zone classification fails for a user who does not have Windows administrator rights. The user is classified to the default or quarantine zone.	Occurs when a Windows device profile is configured on the appliance to check for a certain client certificate on a user's device in either the machine or user store. On an end point device running Windows Vista, the machine store cannot be opened for a user who does not have Windows administrator rights, and the search for the client certificate fails.	61578

ExtraWeb

Symptom	Condition / Workaround	Issue
The Safari browser stops responding when accessing Web sites that use applets.	Occurs after logging in to the appliance in a Safari 4.0.5 browser on a machine running Mac OS X 10.5.8, and accepting the certificate prompts. The certificate prompts show header values instead of strings, which appears to be a browser issue. This issue can occur on all Web sites that use applets.	89190

OnDemand Proxy

Symptom	Condition / Workaround	Issue
The first time a user installs OnDemand proxy, OnDemand proxy might not redirect all connections.	Occurs for connections to unqualified names that are fewer than 16 characters in length, which are not redirected if DNS cannot resolve them. This can happen if no DNS suffix is configured on the system. **Workaround**: Reboot the system. When DNS fails, WINS or WINS Broadcast is used, but WINS cannot perform name resolution until the system has been rebooted.	60633

OnDemand Tunnel

Symptom	Condition / Workaround	Issue
OnDemand Tunnel upgrade appears to work using two different appliances, but activation fails with an error that there is no phonebook.	Occurs when a non-administrator installs OnDemand Tunnel on a Windows system, and when subsequent upgrades are performed using different appliances. **Workaround**: Install OnDemand Tunnel when logged in as an administrator. Upgrade from the same appliance, as administrator or non-administrator.	71411

OPSWAT Secure Desktop Emulator (SDE)

Symptom	Condition / Workaround	Issue
The user may experience Firefox becoming unresponsive or the error message "Couldn't initialize the application's security component error."	Occurs when running Windows Vista 64/32–bit and launching Secure Desktop Emulator using Firefox. The Firefox browser does not launch within SDE and so the client cannot access the WorkPlace home page inside SDE.	98293
Secure Desktop Emulator displays a “Session Terminated” dialog box, but does not exit if the user does not click OK. The WorkPlace session exits properly.	Occurs when running Secure Desktop Emulator and recurring EPC finds a change in the system status that triggers the SDE session to exit.	97901
Web resources are not accessible using the Web Proxy Client (EWPCA) and OnDemand Proxy in the Secure Desktop Emulator.	Occurs when there is already a proxy (.pac file or auto configuration) defined in the Internet Explorer or Firefox browser and the user attempts to modify the preset proxy settings in the secure desktop. **Workaround**: Use OnDemand Tunnel agent or use a manual proxy. Access Web resources using an alias or a custom access option such as a hostname or port mapped URL.	91956, 91954, 91946, 91942
Secure Desktop Emulator does not always start on the first attempt.	Occurs when using a 32-bit Windows 7 machine using Internet Explorer 8 and Java, either when starting it in IE8 with no other browsers running, or when IE8 is running and then Firefox is launched and the user attempts to start Secure Desktop Emulator in Firefox. **Workaround**: Press the F5 key to refresh the browser and then SDE starts.	91939

Symptom	Condition / Workaround	Issue
The rundll.exe process stops responding for a user accessing a realm that uses Secure Desktop Emulator.	Occurs when the user logs in for the first time to the SDE realm from a freshly installed Vista SP2 32-bit machine with Internet Explorer 8 and User Access Control (UAC) turned on. **Workaround**: Log in again, as subsequent logons do not have the problem.	91369
Mapped network drives are not shown in the My Computer window and the share is not available until Secure Desktop Emulator is restarted.	Occurs when a network drive is mapped to a network share while in a Secure Desktop Emulator session. **Workaround**: Exit the SDE session and launch a new SDE session.	91321
Opening an Internet Explorer or Firefox browser after exiting Secure Desktop Emulator results in a warning that the last browsing session closed unexpectedly.	Occurs when an Internet Explorer and/or Firefox browser was open when SDE was launched, and SDE closed the browsers.	91067
The Virtual Desktop background image continues to display after logging off.	Occurs when running windows 7, creating a realm with Translated Mode and SDE enabled, and accessing the WP using the same realm. Allow the agents to install and provision. Once the Virtual Desktop is created, click on 'Start'->'Log off'. Try to connect to the same client using the same user (but do not access the appliance).	90794
Users cannot print from Notepad on Windows 7 and an error message is displayed.	Occurs when a user enables printing out of the Secure Desktop Emulator, and attempts to print from Notepad on a system running Windows 7. **Workaround**: In these instances, the user can print from Microsoft Word, and then try printing from Notepad. Print support for 64-bit systems running Windows Vista or Windows 7 may be developed for future releases.	90759
OnDemand Dynamic Mode, OnDemand Port Map Mode, and Web Proxy Client fail to activate in the Secure Desktop Emulator when using ActiveX.	Occurs when using ActiveX for provisioning on 32-bit and 64-bit machines running Windows Vista SP2 and on 32-bit machines running Windows 7, with User Access Control (UAC) turned on. **Workaround**: Turn UAC off or use Java with Internet Explorer for provisioning and activating agents.	90508
Secure Desktop Emulator does not remove installed applications when it terminates. The application can still be used on the computer, outside of SDE.	Occurs when any application is installed while in a Secure Desktop Emulator session and then the session is ended.	90349
OnDemand Tunnel activation fails with Secure Desktop Emulator when using ActiveX.	Occurs when in a Secure Desktop Emulator virtual desktop on 64-bit machines running Vista SP2 with User Access Control either on or off, and on Windows 7 machines with User Access Control turned off. **Workaround**: Turn UAC on for 32-bit Windows 7 machines and use 32-bit Vista SP2 with UAC either on or off.	90184

Symptom	Condition / Workaround	Issue
The client may experience error messages: "This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator." After clicking OK, the message “Unspecified Error” is displayed by explorer.exe.	Occurs when running Secure Desktop Emulator, then right clicking on the virtual desktop and selecting “Personalize”. This is a known issue with Microsoft Explorer.	90036
Secure Desktop Emulator does not exit upon logging out of WorkPlace, and clicking Logout in WorkPlace displays an error dialog.	Occurs when using a 32-bit machine running Windows 7 and Internet Explorer 8 with User Access Control turned off. This problem occurs because SDE is unable to properly load ActiveX. **Workaround**: Manually exit the secure desktop by accessing the tray icon and clicking Exit.	90019
Browser window does not close after launching a Secure Desktop Emulator session.	Occurs when a user launches a Secure Desktop Emulator session through the Firefox Web browser. The browser window displays a "waiting" message, even once the SDE session has begun.	90016
An incorrect MS VC++ run-time error may be displayed by Internet Explorer.	Occurs when a user successfully removes the Secure Desktop Emulator plug-in using the Internet Explorer browser tools options.	90015

Platform/Operating System

Symptom	Condition / Workaround	Issue
In split tunnel mode, file shares are not always redirected to the appliance. Traffic bound for resources defined on the appliance is redirected through the tunnel, and all other traffic is routed as normal.	Occurs when using Connect tunnel on a Vista computer and an appliance in split tunnel mode. File share access—which uses the SMB protocol—may not be redirected properly if there is a conflicting resource on both the remote and local networks. For example, if Connect tunnel is started on a network at 192.168.144.0/24 and there is a resource at 192.168.144.100, a user who is trying to access a share on a remote network at 192.168.144.100 may get connected to 192.168.144.100 on the local network instead. On the Vista operating system, SMB does not use the appliance's routing table directly, but issues connects on different interfaces simultaneously: whichever connection succeeds first is the one that is subsequently used (even if the routing table on the appliance prescribes something else). In this example, if the 192.168.144.0/24 interface connects first, then access to the resource at 192.168.144.100 will not be redirected.	63383
The Access Manager component fails to properly install on Windows 7 platform clients, causing a dialog box prompt to display a request for the insertion of a smart card.	Occurs because the certificate is not being properly imported in Internet Explorer on Windows 7 systems. **Workaround**: Mark certificate keys as exportable.	85698

Symptom	Condition / Workaround	Issue
SonicWALL Aventail EX7000 and EX6000 appliances refuse to boot during re-imaging.	Occurs when a USB device is inserted into the appliance. During the re-imaging process, appliances boot from the internal hard drive instead of a compact flash card. **Workaround**: Before rebooting an EX7000 or EX6000 appliance, remove any USB devices.	76435

Policy Server

Symptom	Condition / Workaround	Issue
Group affinity checking is not successfully completed with certain authentication scheme combinations.	Occurs when PKI is configured as the primary authentication scheme, and Active Directory, LDAP, or RADIUS is configured as the secondary authentication. **Workaround**: Remove the secondary authentication.	90434

Virtual Assist

Symptom	Condition / Workaround	Issue
The Help button incorrectly displays Windows help.	Occurs on Mac OS X when the Help button is clicked.	94630
The Virtual Assist session sometimes stops responding.	Occurs on Mac OS X when closing the browser window where the initial Virtual Assist session was launched.	94629
The technician application stops responding in certain conditions.	Occurs on Mac OS X after an ungraceful exit if the browser is closed before the application exits. **Workaround**: Exit the application first, then close the browser.	94627
The technician application sometimes stops responding.	Occurs on Mac OS X when the technician application shows the last screen of the Mac system even after ending support.	94626
The customer system reboots and then displays an error message about incorrect parameters. The technician cannot reconnect with the customer.	Occurs when the technician PC is running Windows Vista SP2 with Internet Explorer 8, the customer PC is running Windows XP SP3 with Internet Explorer 8, the technician clicks “Reboot Customer PC”, and the customer provides their credentials. **Workaround**: The customer logs back into the wait queue on a new ticket either by entering the authentication code or by responding to an invitation sent when the technician creates a new ticket.	91774
The Safari browser stops responding after a technician attempts to service a re-queued Windows customer.	Occurs when a technician has both a Windows-client customer and a Mac-client customer waiting for service in the Virtual Assist queue, and the technician services the Windows customer and then attempts to service the same Windows customer again after a re-queue.	90634

Symptom	Condition / Workaround	Issue
The technician cannot start the service for the customer again after re-queue.	Occurs on Mac OS X when the client application is not terminated when the technician re-queues the customer.	90511
Cannot use the same user name to log in as a technician for approximately six minutes.	Occurs on Mac OS X when the technician selects the option to end support (Stop or Remove).	90510
A customer cannot use an invitation link to join the queue until after six minutes.	Occurs when a customer accepts an invitation to join the Virtual Assist queue for service when it is full, which prompts to try back later, and then tries to use the same invitation link to join the queue after a space opens up.	89674
The technician's screen may momentarily go blank the first time the technician attempts to view the customer screen.	Occurs when a technician initiates a Virtual Assist session with a customer, and selects the full-screen mode option to view the client's screen. **Workaround**: The technician and user should each move their mouse to refresh the VNC connection.	88498
During a Virtual Assist support session, Virtual Assist may stop responding while transferring files.	Occurs when the client or customer attempts to send numerous files to the technician's system at one time, using the file transfer tool.	88628

Web Translation

Symptom	Condition / Workaround	Issue
Edited layout is not reflected on Domino Web Access home page after saving the selected layout.	Occurs when using port mapped or host name mapped access for Domino Web Access, and the user edits the layout of the page. **Workaround**: Click the Refresh button to display the new layout.	83358
Using the Windows Explorer style view on SharePoint causes a long delay and then fails.	Occurs when Explorer View is clicked to view a document library on a backend SharePoint server (2003/2007) while logged in through the EX-Series appliance. This is a known limitation due to SharePoint use of built-in URLs with proprietary components. **Workaround**: Use other views that provide tables and columns.	60916

WorkPlace

Symptom	Condition / Workaround	Issue
Clicking OK on a “File Size Exceeded” window closes the window without returning to the folder.	Occurs when a user is logged into WorkPlace using Internet Explorer 8, and attempts to upload a file exceeding the size limit. When the user clicks OK, the warning window sometimes closes without returning the user to the folder containing the file to upload. **Workaround**: Use another type of browser or a different version of Internet Explorer.	83150

Symptom	Condition / Workaround	Issue
Cannot cancel installation of Aventail Access Manager.	Occurs when a file download dialog opens during installation of Aventail Access Manager (the provisioning and EPC component for Windows). If the user clicks Cancel in this dialog box, the Aventail Access Manager Web page does not display any navigation buttons. **Workaround**: Refresh the browser, and the buttons used to select the installation options will display.	61369
Certificate authentication process stalls during login to WorkPlace.	Occurs when you attempt to log in to a realm that requires a client certificate when connecting to WorkPlace using Internet Explorer on a PDA that is running Windows Mobile 5. **Workaround**: Click the **Next** button.	61269

Resolved Issues

This section describes resolved issues for this release. The five-digit numbers in brackets are internal tracking IDs. The issues are organized into the following categories:

AMC Configuration

Symptom	Condition / Workaround	Issue
The client may only have the Outlook Web Access 2003 Web agent Single Sign On profile.	Occurs when the client has OWA 2003 and needs to upgrade to OWA 2007 and OWA 2010.	96887
The Aventail Management Console may have validation errors causing it to become unresponsive.	Occurs when defining a resource variable within a network share resource.	96285
The client is unable to remove an added resource.	Occurs when trying to remove added resources created by the client that are no longer in use.	95727
The following error message is displayed "One or more selected layouts is in use and could not be deleted."	Occurs when trying to remove an added layout created by the client that is no longer in use.	95723
Unable to apply pending changes and the following error message is displayed "Caught exception while trying to apply changes: org.xml.sax.SAXParseException: Character reference "&#0" is an invalid XML character"	Occurs when using a wild card certificate signed from a certifying authority. The administrator is able to import the certificate to the management console. However, while binding or using the certificate for WorkPlace, AMC displays an error that prevents the system from applying configuration changes.	95145
The primary authorization server username is logged instead of the secondary authorization server username.	Occurs when enabling “RADIUS accounting” and "Audit username from this server" for the secondary authorization. This condition only happens when the usernames for both servers are different.	90384

Authentication

Symptom	Condition / Workaround	Issue
A “page cannot be displayed” error message is seen.	Occurs when upgrading to SonicWALL Aventail E-Class SRA EX-Series 10.5.2, then authenticating to WorkPlace. The policy server becomes unresponsive and requires a restart.	96685
The SonicWALL Aventail E-Class SRA EX-Series accepts authentication and allows access to the system, even though an error “48” is displayed.	Occurs when configuring the Lightweight Directory Access Protocol authentication server on SonicWALL Aventail E-Class SRA EX-Series. Authenticating a valid username with an invalid password functions properly and denies access, but when the password is removed and authentication is requested, access is still granted.	94922
The following error message is displayed: “your password will expire in --15529 days”.	Occurs when using SonicWALL Aventail E-Class SRA EX-Series 10.0.4, launching the Connect Tunnel client and requesting authentication. If the error message, “your password will expired in --15529 days” appears, select the “continue” option.	94758

Certificates

Symptom	Condition / Workaround	Issue
The Secure Socket Layer Cipher Suites are restricted in the SonicWALL Aventail Management Console.	Occurs when upgrading to SonicWALL Aventail Management Console 10.5.2. The Secure Socket Layer Cipher Suites are disabled for the Digital Security Standard signature, causing the system to not function properly without regenerating the Secure Socket Layer certificate with the RSA signature.	96195

Connect Mobile

Symptom	Condition / Workaround	Issue
The client’s network connection drops after an extended period of time.	Occurs when the client is using an iPhone/iPad with ActiveSync and Evolved Packet Core is enabled. Enabling EPC will cause the symptom to repeat itself.	94633

Connect Tunnel (CT)

Symptom	Condition / Workaround	Issue
The client may experience issues with the Encapsulated Security Payload.	Occurs when running Windows 64–bit with a 3G card or DSL home Internet connection. The Encapsulated Security Payload may not initiate when using Connect Tunnel.	98188
Connect Tunnel may become unresponsive and require a restart.	Occurs when trying to log into a realm with AD certificate as the primary and AD Username/Password as the group affinity server. This can cause the Connect Tunnel to become unresponsive.	96628
The user is unable to customize Connect Tunnel.	Occurs when installing Connect Tunnel from WorkPlace. Once the Connect Tunnel installation is complete, the “ngsetup.ini” file is deleted.	96461
Linux Connect Tunnel/On Demand Tunnel might not work with Turbolinux 7.	Occurs when running Linux Connect Tunnel/On Demand Tunnel with Turbolinux 7.	96415
The Connect Tunnel DNS filtering code may cause the system to become unresponsive and require a restart.	Occurs when the Connect Tunnel DNS attempts to handle the EDNS0 records, but is unsuccessful.	96086
The system becomes unresponsive and displays the message: "Establishing VPN Connection..."	Occurs when establishing a Virtual Private Network Tunnel, after the user has logged into the system.	96060
The user may not be able to connect to SonicWALL Aventail Management System.	Occurs when running Windows 7 with Qualcomm Gobi aircards. Wired connections and other network cards are working properly, but the Qualcomm Gobi aircard is having connection issues.	95798
The Operating System static route might not be added to the client machine.	Occurs when running Windows 7 and enabling Connect Tunnel. The route is not added and the client may not be able to provide remote support.	95718
Any Fully Qualified Domain Name with “intl.warnerbros.com” is not redirected across the Virtual Private Network Tunnel.	Occurs when using “redirect all + local” from an international domain machine (primary Domain Name Server int.warnerbros.com). The client primary DNS suffix is not excluded from the redirection.	95201
Any Fully Qualified Domain Name with “domain.com” is not redirected across the Virtual Private Network Tunnel.	Occurs when using “redirect all + local” from a machine with a primary Domain Name Server of “domain.com”. This extension should give the administrator the power to change behavior, such that “domain.com” connections are considered remote and are redirected across the tunnel while in “redirect all + local”.	95200

Symptom	Condition / Workaround	Issue
New clients are unable to authenticate using Connect Tunnel.	Occurs when running SonicWALL Aventail E-Class SRA EX-Series 10.0.3-042 and attempting to authenticate with Connect Tunnel. New clients are denied access to Connect Tunnel, but existing clients are allowed access.	94798
The client may experience loss of Domain Name Server capability.	Occurs when running Mac OS 10.6.x with the OnDemand Tunnel and Split Tunnel access methods. Accessing the internal intranet using a Fully Qualified Domain Name as the URL may not work, but when using an IP address the system functions properly.	94687
Virtual Network Computing (VNC) can be used to illegally access the client's Virtual Private Network.	Occurs when an unauthorized source gains access to the Virtual Private Network Tunnel. This puts the client in a situation to become an intermediary for unauthorized access to the Secure Socket Layer VPN. Once in the VPN, the unauthorized source will have access to the default gateway, DHCP and DNS servers.	94498
The client may experience a software update message for Connect Tunnel.	Occurs when running Apple or Linux OS and establishing a Connect Tunnel session. The appliance displays an update message even though the Connect Tunnel is set for manual update.	89490
The ngutil log is not Displayed in English.	Occurs when running the ngutil log in the Japanese language and selecting the command "MODE CON CODEPAGE SELECT = 437". The command line log is not converted to English, but is changed to a non-readable format. If the ngutil log is exported, the Japanese format still appears in the exported log.	65479

End Point Control (EPC)

Symptom	Condition / Workaround	Issue
The client may be running an outdated version of OPSWAT.	Occurs when running the older version of OPSWAT. The client should upgrade to the latest version of OPSWAT.	97303
The user system may not display the desktop background image.	Occurs when the Uniform Resource Identifier in ODIS.ini (the Secure Desktop Emulator initialization file) is relative to the eth1 IP address.	97140
The user may experience the EPC becoming unresponsive.	Occurs when running Mac OS and installing any version of McAfee Anti Virus. Creating a profile which checks for the DAT file update age can cause EPC to become unresponsive.	96806
A JPEG image which contains a warning message is not displayed correctly.	Occurs when switching configurations from Anti Spam Desktop to Secure Desktop Emulator. The warning message is visible when the SDE is loading. Once loaded, the message does not appear. The warning message should appear on the secure desktop even after the SDE is done loading.	96283
The user may experience classification issues when connecting to ActiveSync.	Occurs when Setting up an 'EquipmentID - Registered' standard zone with a device profile for ActiveSync. Upon initial connection the zone which checks the device- ID's is still only working once the phone has made an initial connection from the default zone. This allows any valid user to access the Exchange server, without having the device ID checked.	96145
The client may experience the error message “Your session has been idle too long. Please close your browser and log in again”.	Occurs when running Mac OS 10.6.x and logging into a Windows Phone with the Connect Tunnel client access restricted for the zones under EPC.	95772
The user may not have access to restrict the “writing” function on the CD drive.	Occurs when running SonicWALL Aventail Secure Desktop and data is written to the CD +RW OR DVD +RW. The client should be able to configure SDE to enable or disable write access to the CD drive.	95175

ExtraWeb

Symptom	Condition / Workaround	Issue
Japanese clients may receive the error message "Invalid UTF-8 encoding in URL".	Occurs when using Outlook Web Access to translate languages.	98168
The error message "Tunneling Failed for srvInfo<" + this.d + ">") may not communicate the error status back to the main OnDemandApplet.java.	Occurs when the client tunnel Java applet displays the status of the tunnel. The error message should report back to the main OnDemandApplet.java.	97746
The client may only receive "web" access in place of "web and client/server access".	Occurs when using a local proxy file with Internet Explorer on Windows 7. This occurs because the redirect.pac file is not overwriting the local proxy file.	97553
The client may experience warning messages every 8 minutes on the appliance.	Occurs when running SonicWall Aventail Management Console 10.5.2 and configuring Active Directory as a backend server for authentication.	97093
The client may experience the error message “error 302”.	Occurs when upgrading to SonicWall Aventail Management Console 10.5.2 and accessing Apache2 web application from WorkPlace. Once the credentials are entered, the page is redirected to error “302” and the web application becomes unresponsive.	96765
The client may be unable to end inactive user sessions.	Occurs when the Extra Web connection does not time out after a period of inactivity. The system should ask for authentication after a time out has occurred.	96688
The client may experience the following error message "Excel Found unreadable content in 'xxxx.xls'. Do you want to recover the contents of this workbook? If you trust the source of this workbook, click Yes."	Occurs when using the Web Translated access method to configure and access the internal URL resource (Livelink Document Application). Excel files (only .xls format) downloaded from this URL resource appear corrupted and the user gets an error message while opening Excel documents.	94963

EVPN

Symptom	Condition / Workaround	Issue
The user may get disconnected from Connect Tunnel.	Occurs when enabling the recurring EPC function and logging into Connect Tunnel. The session may disconnect within a 45 minute time frame. If the recurring EPC function is disabled, Connect Tunnel will not disconnect the client.	95167

Kernel (Platform OS)

Symptom	Condition / Workaround	Issue
Some users are not able to reach the back end resources.	Occurs when connecting to the appliance via Connect Tunnel and pinging the backend resource from the SSH console or AMC. An error message “No buffer space available” appears.	95008

Linux Platform

Symptom	Condition / Workaround	Issue
The user may experience the following error message “Interface eth0 on Aventail-viper-2500-2 is Unknown”.	Occurs when using a Solarwinds SNMP server to monitor all appliances. Every day at 6:28, the interfaces on the appliances do not respond to pings.	98133
The user appliance can become unresponsive and require a restart.	Occurs when running SonicWALL Aventail Management Console 10.0.5 with clt-hotfix 10.0.5-003 and pform hotfix 10.0.5-002.	96587

Logging

Symptom	Condition / Workaround	Issue
The client may experience the following error message “FATAL Error AVPSD kcomm notify: 3 failed: 22 (Invalid argument)”.	Occurs when viewing the system message log. The error message is labeled as “FATAL” but it should be labeled “WARNING”.	96710
The Management Audit Log and Policy Audit Log do not log any data.	Occurs when upgrading to SonicWALL Aventail Management Console10.5.x and viewing the log data. Changing the setting on the appliance should cause data to be stored in the logs.	95832

NAM

Symptom	Condition / Workaround	Issue
The client may not be able to access the system when a username contains an underscore.	Occurs when using SonicWALL Aventail Management Console 10.5.1 and accessing the system using a Domain Name System name. If entering an IP address the system functions properly.	95757

Policy Server

Symptom	Condition / Workaround	Issue
The Citrix server farm links are always visible to all clients.	Occurs when upgrading to SonicWALL Aventail Management Console 10.0 and logging into the system. It is expected that the Citrix server farm links are shown only if the client can access the underlying resources.	96204

Provisioning

Symptom	Condition / Workaround	Issue
Internet Explorer 9 and Firefox 4 are not recognized by the provisioning code.	Occurs when testing SonicWALL Aventail Management Console 10.5.3 with browsers Internet Explorer 9 and Firefox 4. The system needs to be updated to detect internal code and recognize these new browsers.	97389
The user may be experiencing possible vulnerability issues.	Occurs when creating an absolute path name based on values in the "CabURL" and "Location" arguments and can be exploited to cause a stack-based buffer overflow.	94634
All access methods/agents cannot be supported by Windows 7.	Occurs when running Windows 7 SP1 (x86/x64) with SonicWALL Aventail Management Console 10.5.3. The access methods/agents need to be supported on this operating system.	93033
The user may not have support for Safari 5.0 web browser.	Occurs when running Mac OS, using the SonicWALL Aventail Management Console 10.5.3 and accessing the Safari 5.0 web browser.	93032
The user may not have support for new versions of Sun JRE 1.6.0 update 21 or higher.	Occurs when running the Java 6 Update 22 with Internet Explorer and Firefox web browsers.	93031
The user may experience all access agents (Translate, EWPCA, OD Proxy and OD tunnel) not functioning properly.	Occurs when running Internet Explorer web browser with SonicWALL Aventail Management Console 10.5.x.	92542
The user may not have support for new versions of Firefox web browser.	Occurs when running Firefox web browser with SonicWALL Aventail Management Console 10.5.3.	92265

User DB

Symptom	Condition / Workaround	Issue
Replacing a node can cause session_id numbers to be reused, resulting in the system becoming unresponsive and requiring a restart.	Occurs when replacing a High Availability node, after a large database has already been created.	96809

Workplace

Symptom	Condition / Workaround	Issue
The user's WorkPlace session might end unexpectedly.	Occurs when activating an On Demand Tunnel. The Workplace Details option may end the user session.	96286
The client may experience the Single Sign On function becoming unresponsive.	Occurs when updating SonicWALL Aventail Management Console 10.5.2 and activating the Single Sign On function. The cookie path for the SSO is not correct. It is sending SharePoint in the cookie path when it is supposed to send Outlook Web App.	95683
The client may be unable to access the File Share resource through WorkPlace, which can cause the system to become unresponsive.	Occurs when upgrading to SonicWALL Aventail Management Console 10.5.x and accessing the File Share function.	94796

Technical Documentation and the Knowledge Portal

Check the SonicWALL Customer Support Knowledge Portal, available when you log in to MySonicWALL, for information and hotfixes that are relevant to your appliance.

Technical documentation is available on the SonicWALL Technical Documentation Online Library:
http://www.sonicwall.com/us/Support.html

Last updated: 3/18/2011