Release Notes

Secure Remote Access | **SonicWALL Aventail E-Class SRA EX-Series 10.5.2**

Platform Compatibility

The SonicWALL Aventail E-Class SRA EX-Series 10.5.2 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 Safari 5.0.x.

Upgrading from Earlier Versions

If you are upgrading a SonicWALL Aventail E-Class SRA EX-Series appliance to version 10.5.2 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

1. The **OPSWAT Secure Desktop Emulator** is currently provided as a beta-quality release and has a number of known issues. Details about this feature are provided in the next section.

2. 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:

- **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.
- **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.
- **OPSWAT Secure Desktop Emulator (SDE) –** Provides VPN administrators with an additional end-point data protection tool that prevents end users from copying or moving data from an end-point system to other locations that have not been qualified for security clearance. When a client device is classified into a zone that requires the desktop emulator, the emulator will automatically deploy for the user.

  The Secure Desktop Emulator is available as a beta-quality feature for 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

  Note: SonicWALL recommends using Java with Internet Explorer when using SDE.
- **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 2008 Server
    - Mac OS X 10.5 (Leopard)
    - Mac OS X 10.6 (Snow Leopard) (32-bit, 64-bit)

Known Issues

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

AMC Configuration

Symptom	Condition / Workaround	Issue
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
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

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
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

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 user’s 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

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
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

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
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
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

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
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
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
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

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
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
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
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
AMC displays “Unknown” for some entries in the unregistered devices log table.	Occurs because activeSyncMobile enumeration is missing from the platform row in the MySQL database equipmentIdentifier table.	93530

Authentication

Symptom	Condition / Workaround	Issue
After authentication, a message is displayed which says "Your password will expire in -24626 days (Numbers appear randomly generated).	Occurs when Active Directory is misconfigured and is giving incorrect timestamps.	93749
Users not in Active Directory are incorrectly granted access for rule with Dynamic Group Expression.	Occurs when using RADIUS as primary authentication with Active Directory group affinity check enabled.	92336
One Time Password user login session does not timeout after 15 minutes.	Occurs when the user is inactive for 15 minutes or more.	90263

Cache Cleaner (OPSWAT CC)

Symptom	Condition / Workaround	Issue
Cache Cleaner cannot be disabled on a Mac OS X 10.6 machine.	Occurs when the CC system tray icon is right-clicked and the Disable option is selected. Upon exit, CC still removes all session related information. This occurs when logged into WorkPlace on a Mac OS X Snow Leopard system with a Safari 4.0 browser.	88991

Cache Cleaner is not provisioned on some platforms when Secure Desktop Emulator is configured.	Occurs on non-Windows client machines when Secure Desktop Emulator (SDE) has been enabled in the appliance configuration. SDE is not supported on non-Windows platforms, so to maintain legacy support, CC needs to be provisioned.	86749

Certificates

Symptom	Condition / Workaround	Issue
PKI authentication through Connect Tunnel with a chained certificate fails and displays an Access Denied message.	Occurs when the PKI server is configured with the primary CA, the “sec1” intermediate CA, which is issued by the primary CA, is installed in the client machine browser, and then Connect Tunnel is installed and a login is attempted with a secondary user certificate issued by the sec1 CA.	93921
Only one certificate is displayed when a user is prompted to choose among multiple certificates.	Occurs when using multiple certificates and the common name (cn) field is identical.	91874

Connect Tunnel (CT)

Symptom	Condition / Workaround	Issue
Remote Internet Proxy does not always work.	Occurs when the PAC file is sent as chunk-encoded stream.	92559
Connect Tunnel client picks the wrong one among multiple client certificates with the same common name and eventually authentication fails.	Occurs when multiple valid certificates are imported on the client machine's browser in such a way that two client certificates have the same common name but are issued by different CAs.	92005
The Connect Tunnel system tray icon takes a couple of minutes to respond, soon after Connect Tunnel connects.	Occurs when an internal recurring EPC request times out, causing the delay.	91763
Authentication fields are grayed out on Windows 7 after installing Connect Tunnel with the ngsetup.ini file.	Occurs when logged into Windows 7 as a non-administrator, after installing Connect Tunnel while logged in as an administrator and then logging out.	91493
Connect Tunnel Windows 7 users cannot get to any destination without a route, although other clients can.	Occurs when using split tunnels.	91272
Connect Tunnel retains the fallback connection profile after disconnecting, instead of reverting to the primary appliance connection profile.	Occurs when Connect Tunnel connects to the fallback appliance when the primary appliance is not available, and then there is an unexpected disconnect to the fallback connection (client machine loses Internet connectivity or secondary appliance becomes unreachable).	90853
Connect Tunnel fails to automatically re-establish a connection after trying to connect to a unit.	Occurs when the unit has just been upgraded from an older version of firmware to a newer version of firmware.	88143

End Point Control (EPC)

Symptom	Condition / Workaround	Issue
Users fall back to the default zone for the first time with iPhone ActiveSync.	Occurs when setting up ActiveSync on the iPhone (3G, 3GS & 4) and attempting to do the initial sync using GPRS.	93870
Mac/Linux Client libraries and AMC need upgrade to OPSWAT version 3.4.15.1.	Occurs when running older OPSWAT versions.	93712
Windows Client libraries and AMC need upgrade to OPSWAT version 3.4.15.1.	Occurs when running older OPSWAT versions.	93711
Advanced EPC for Mac users classifies users incorrectly to the default zone.	Occurs when several AntiVirus definitions are used in the EPC profile assigned to the EPC zone, and the AntiVirus installed on the Mac client machine is not the first one declared inside the EPC profile.	92305
EPC fails intermittently on Verizon or Sprint aircard based connections resulting in users being classified to the default zone.	Occurs when the realm is configured to allow OnDemand tunnel along with an EPC check for McAfee Enterprise Antivirus and a domain check with approximately 15 NetBIOS Domain names are specified in the profile.	91151
The initial classification of ActiveSync based connection requests puts the device in the default EPC zone when using EquipmentID.	Occurs on the initial request because the Equipment ID is empty. Subsequent requests include the Equipment ID and are properly classified.	88417

ExtraWeb

Symptom	Condition / Workaround	Issue
Upload to Sharepoint via Web proxy fails in Vista and Windows 7.	Occurs when attempting to upload a file larger than 30 KB with Internet Explorer 8.	94197
Appliance does not accept new connections through ExtraWeb, Connect Tunnel or WorkPlace version 10.0.3 and Apache core dumps, requiring an appliance reboot.	Occurs when using a load balancer in front of three EX-2500 appliances, each licensed for 2000 users.	93481
After upgrading from version 9.0.2 to 10.0.3, the SAP application URL configured on the start page for an additional WorkPlace site does not seem to work or goes into a loop.	Occurs when accessing WorkPlace through Internet Explorer 6, 7, or 8. Does not occur when using Firefox.	91492
The user is not redirected to the HTTPS Web site for a resource after using HTTP instead of HTTPS, but is redirected to the WorkPlace site.	Occurs when the user tries to access a hostname mapped resource using HTTP instead of HTTPS, and the certificate is not a wildcard certificate.	89864
SSO does not work for an intranet Web application, and the user is prompted for credentials.	Occurs when the application is hosted in Microsoft SharePoint Team Services using SharePoint 2007 on Windows Server 2008. Also the backend resource is configured to accept only NTLMv2 messages.	89319

Accessing an Outlook Web Access 2010 resource displays the login page, but then reports that the credentials are invalid.	Occurs when the OWA resource is accessed in Translated mode. When the OWA resource is configured on the appliance, an alias name is configured. Users log in to WorkPlace to access the OWA resource.	87501

Logging

Symptom	Condition / Workaround	Issue
Rebooting an appliance with a very large troubleshooting database takes a long time.	Occurs when the MySQL database size is well over 1 gigabyte.	93933
Logserver process consumes too much memory.	Occurs due to a memory leak.	91698

OnDemand Proxy

Symptom	Condition / Workaround	Issue
OnDemand proxy users can see an error when they try to access WorkPlace.	Occurs after upgrading the client system from Vista to Vista SP1. **Workaround**: Uninstall OnDemand proxy either before or after the upgrade to Vista SP1, and reinstall OnDemand after the upgrade.	68628

OPSWAT Secure Desktop Emulator (SDE)

Symptom	Condition / Workaround	Issue
Secure Desktop Emulator leaves the client system in a state in which no desktop icons appear, the browser does not open, and other problems occur.	Occurs when Secure Desktop Emulator exits due to an inactivity timeout while the computer is locked, and then the user unlocks the computer and attempts to use it. **Workaround**: Reboot the client computer.	91941
Explorer.exe in Secure Desktop Emulator stops responding.	Occurs when trying to copy a file from a network share to the secure desktop on a Windows XP SP3 machine with Internet Explorer 8.	91010
The background image for the secure desktop disappears.	Occurs when the browser instance created in the secure desktop is minimized. The browser instance is created in the secure desktop when WorkPlace is launched in a browser to access a realm with translated mode and Secure Desktop Emulator enabled. This issue occurs on a 64-bit machine running Windows Vista and using Internet Explorer 8. **Workaround**: Switch to the normal desktop and then switch back to the secure desktop.	90870

Firefox becomes unresponsive and a dialog box in the secure desktop displays the message: "Firefox is already running but is not responding. To open a new window, you must first close the existing Firefox process or restart your system." Clicking OK has no effect. Attempting to open another Firefox browser in the same session causes the same message.	Occurs when using a Firefox 3.5.9 browser to launch WorkPlace to access a realm with translated mode and Secure Desktop Emulator enabled. This occurs on a 64-bit machine running Windows Vista SP2 when logged in as the administrator.	90817
With a proxy configured, the Secure Desktop Emulator loads very slowly and all the operations within the secure desktop slow down further.	Occurs when using Windows XP SP3 with Firefox or Internet Explorer 8, with a proxy configured (manual proxy, Proxy Auto-Config (PAC) file, and auto-proxy).	90593
The right-click menu is slow to display in the Secure Desktop Emulator. It does not appear for approximately 30 seconds when using Internet Explorer, and approximately 45 seconds when using Firefox.	Occurs when you right-click in the secure desktop.	90587
A dialog box with the message, "Your session has been terminated because of a change in your system status. Please contact the administrator for more information." can be displayed in the normal desktop and the user in SDE will not be aware of it. If the user clicks on any link in WorkPlace, the SDE session will end.	Occurs when there is a change in the device profile and recurring EPC is enabled.	90562
Within Secure Desktop Emulator, created files or folders display lock icons.	Occurs when a Windows 7 user creates any files or folders under any of the drives such as C:\ or D:\, and views them as a list.	90198
In Secure Desktop Emulator, folders with lock icons in root drive are displayed in all other drives.	Occurs when folders are displayed with lock icons in the C:\ drive (which is the root drive), and then viewing the D:\, E:\, or other drives, and the window that is displayed after inserting a USB flash drive. This occurs on Windows 7.	90197
Some folders under the root drive are displayed with lock icons in the secure desktop.	Occurs when the contents of the C:\ drive (on which the OS is installed) are viewed as a list in the Secure Desktop Emulator virtual desktop. This includes the Users, Windows, Program Data, and other folders. This occurs on Windows 7.	90195

Platform/Operating System

Symptom	Condition / Workaround	Issue
New users cannot connect after memory and swap space utilization reaches 90% or above.	Occurs on a cluster when hundreds of users are RDP access via WorkPlace.	93091
Appliance reboots every 4 to 5 hours as the user load increases.	Occurs after upgrading to version 10.0.4 and installing the pform-hotfix-005 on 13 appliances that are deployed behind a load balancer, with around 9000 resources defined.	92625

Memory utilization increases until appliance stops accepting new connections and eventually generates core files. Connect Tunnel users who are connected will not be able to access various resources at the backend.	Occurs when memory utilization reaches 60% to 70% due to excessive memory usage or leaking by the policy server in relation to LDAP.	91975
The user sees a script error and cannot access WorkPlace through Internet Explorer.	Occurs when Java is installed on a client computer running Vista, but ActiveX and Java are disabled. This causes Internet Explorer 7 to fail to use Translated Web access. **Workaround**: Enable Java or ActiveX. Works with IE8.	63132
Users cannot type in a new mail window to compose a message in Outlook Web Access.	Occurs when using Windows Internet Explorer 7.0 and Microsoft OWA Exchange 2003 on a client computer running Vista. **Workaround**: Refer to the following Microsoft knowledge base article for instructions on installing a patch on your Microsoft Exchange Server 2003 that addresses this issue: http://support.microsoft.com/?kbid=924334 This is fixed in Exchange 2007.	63044

Policy Server

Symptom	Condition / Workaround	Issue
LDAP users are unable to change passwords from WorkPlace.	Occurs after upgrading the appliance to version 10.0.4 from 10.0.2, without LDAP over SSL option enabled.	92056
A DNS query is sent by the appliance to the primary DNS server whenever there is an AMC change, and causes errors for WINS in the logs.	Occurs when the query is made with a comma separating the WINS server IP addresses, which is an invalid format. This is an issue in WorkPlace Network mapping service. When AMC is configured with both primary and backup WINS servers, WorkPlace fails to parse backup WINS server from the properties and instead broadcasts NetBIOS queries on "<primary>,<backup>" for enumerating the network.	91905
Connect Tunnel authentication outage on primary node of HA pair, and the policy server and Apache generate core files.	Occurs due to memory leaks in the policy server.	91526
Deny rule based on group blocks all users.	Occurs when using LDAP/AD group affinity with RSA as the primary authentication type.	91268

Provisioning

Symptom	Condition / Workaround	Issue
ActiveX Control format string overflow allows remote exploitation in which an attacker can execute arbitrary code within the security context of the targeted user.	Occurs when logging input data like team or configuration string.	91522

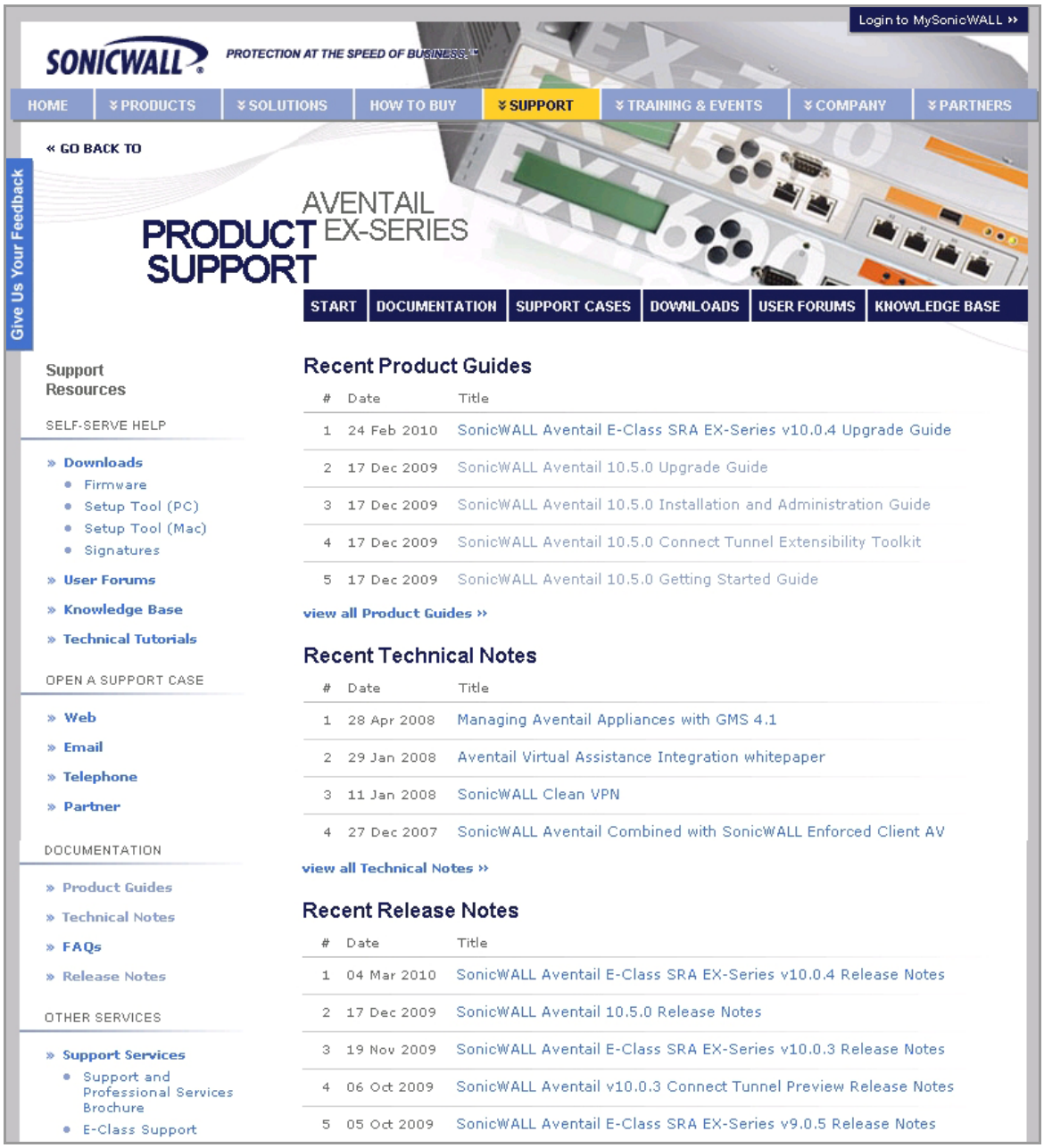
WorkPlace

Symptom	Condition / Workaround	Issue
Bookmarks saved by anonymous users are not displayed in WorkPlace.	Occurs when users are logged in to WorkPlace using the NULL authentication realm. Any bookmarks that they create and save will not display on the WorkPlace home page.	91903, 90819
Users must enable a module extension mechanism for protection against Slowloris HTTP Denial of Service attacks.	Occurs when protection is needed against Slowloris attacks. Slowloris can cause a Denial of Service (DoS) by sending partial HTTP requests to Web servers. These partial requests consume unusual amounts of resources (in the form of open connections), which cause Apache, and other Web servers, to be monopolized quickly. **Workaround**: Users can enable a configuration extension mechanism, "mod_qos". This module does provide Quality-of-Service for web applications running on Apache servers, and may affect performance in some cases. Users must enable this module extension mechanism, as it is not implemented by default in version 10.5.2.	90659
OnDemand access agent and other programs that connect to IP addresses that are in the loopback address range (127.0.0.x) to redirect and secure traffic through the appliance may display an error message that says that you cannot establish a connection.	Occurs on a computer that is running Microsoft Windows XP SP2. **Workaround**: Install the KB884020 update patch from the Microsoft site: http://support.microsoft.com/kb/884020/	61746

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: 10/7/2010