

Release Notes

Version 10.0 is an early release: it has been thoroughly tested internally and in an external beta, but has seen limited deployment in the field. The general release (version 10.0.1) will follow in Q1, 2009.

Contents

- Platform Compatibility
- Upgrading from Earlier Versions
- What's New in this Release
- Known Issues
- Issues Fixed in this Release
- Related Technical Documentation

Platform Compatibility

The SonicWALL Aventail E-Class SRA EX-Series v10.0 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-1500
- SonicWALL Aventail E-Class SRA EX-750

Upgrading from Earlier Versions

If you are upgrading a SonicWALL Aventail E-Class SRA EX-Series appliance to version 10.0 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 www.mysonicwall.com Web site.

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:

Appliance hardware: SonicWALL offers two new E-Class appliances for Secure Remote Access (SRA)—the SRA EX7000 and the SRA EX6000.

Improved appliance setup: For all appliance models except the EX-750, you can specify basic settings using the controls on the front of the appliance, and then run Setup wizard, which is now more complete.

Improved AMC workflow: On a single page in AMC you can now see the big picture—the authentication server and communities that are associated with a realm, and what WorkPlace sites, zones, and access agents are associated with each community. You have direct access from this page to any element in these relationships.

Troubleshooting: Monitor, troubleshoot or terminate sessions on your appliance or HA pair of appliances. You can sort through the list of **User Sessions**—filtering them by user name, realm (authentication server), community, access agent, traffic load, and so on—and then get a quick summary of the details associated with particular sessions.

Active Directory sub-domains: When configuring Active Directory authentication, you can now query sub-domains for user authentication and authorization. During login, the user either enters the domain name, or chooses from a dynamic or static list of domains.

RSA ACE/Server support: The appliance now supports direct connection to an RSA ACE Server authentication for token-based user credentials. Use of the RADIUS interface is no longer required.

Release Notes

WorkPlace portal customization and changes: Basic WorkPlace customization using AMC now includes items like page layout, a tabbed display, or one with a navigation bar along the side. The shortcuts displayed to a community of users can now be defined independent of policy permissions. In addition, the shortcuts can be grouped and arranged per community. Access to portal features such as personal bookmarks can also be controlled on a per-community basis. Administrators who want to have the WorkPlace adhere to corporate Web standards and templates can do advanced customization, modifying the style sheets that ship with the product.

Agent provisioning improvements: When a user logs in to an appliance using OnDemand Tunnel or the OnDemand proxy agent, the system update—if needed—begins automatically.

Connect Tunnel network awareness: The connection between devices and the appliance can handle interruptions—such as suspending a session and later resuming it, or temporarily losing connectivity—without requiring that users reauthenticate, provided the device is using the same IP address. (You can enable roaming—allowing users to resume sessions from a different IP address—when you define your zones.)

Macintosh and Linux Connect Tunnel parity: The Macintosh and Linux tunnel clients have expanded End Point Control capabilities and now support the same authentication methods as the Windows version.

Mac OS X 10.5 support: Full support for Mac OS X 10.5 (Leopard) from Apple.

Policy variables: You can define resources using variables that are based on session properties (such as the IMEI identifier associated with a mobile device), or based on the results of an LDAP query.

One-time password: On LDAP and Active Directory servers you can now configure authentication to use one-time passwords. This offers a more secure, two-factor logon: in addition to a user name and password, the user submits a randomly generated single-use password that is sent via email.

Recurring EPC: Client systems are usually checked for required security features, such as a firewall and antivirus software, when users log in. You can now re-check those clients periodically on a per-zone basis.

Apply or remove hotfixes in AMC: Installing a system hotfix, or rolling back to a previous version, can now be done in AMC.

User-specific redirection rules: For each resource you define in AMC, there is a corresponding routing rule that is sent to clients that redirects access requests through the appliance. Prior to v10.0, all routing redirection rules for all resources were sent to every client system, regardless of whether the user had permission to actually access all resources. In this release, the set of routing redirection rules sent to each client is limited to those that correspond to resources the user has permission to access.

GMS and ViewPoint integration: The integration between SRA EX-Series appliances and SonicWALL's Global Management System (GMS) has been improved. The SRA management console has been integrated into the GMS application and can now send more complete log data to GMS for storage and report generation.

Translation improvements: URL translation now supports viewing and editing data on existing SharePoint 2007 pages. (Administering a SharePoint site, however, is not supported using translation: it requires an agent such as Web proxy.) Domino Web Access 7 will be supported beginning in version 10.0.1.

Citrix/Remote Desktop Protocol improvements: The E-Class SRA series now supports the RDP 6 client and an enhanced provisioning mechanism.

Limit users to a certain number of sessions: You can restrict the number of sessions a user is allowed to use at the same time.

NTLMv2 support added: The E-Class SRA appliances now support NTLMv2 authentication for access to Web resources.

Expanded EPC device profile attributes: The list of attributes available for creating device profiles that establish a trust relationship with a client device has been expanded: profiles for Windows Mobile devices can now use the IMEI number as an attribute, and there is an expanded list of attributes from which to choose for creating profiles for Macintosh and Linux devices.

Release Notes

OnDemand proxy changes: Prior to version 10 of the SonicWALL Aventail E-Class SRA EX-Series firmware, the OnDemand proxy agent provided access to resources protected by the Web proxy service. This agent and its settings are still available to you if you are upgrading from a previous version of the firmware; new customers will use OnDemand Tunnel instead.

Support removed: The v10 release no longer includes the following items. If you have an earlier version of the SonicWALL Aventail firmware that includes any of these items, you can export its configuration file and import it to an upgraded appliance, provided the older firmware predates the newer one by no more than three versions:

- CA eTrust SiteMinder is not supported in this release; only an RSA ClearTrust server can be configured for single sign-on. SiteMinder support will be reinstated in a later release.
- WholeSecurity Confidence Online (from Symantec) and Zone Labs Integrity Clientless Security are third-party client integrity products that are no longer supported.

Known Issues

This section describes the known issues for the firmware for this release. The five-digit numbers in brackets are internal tracking IDs.

Platform/Operating System

Windows XP SP2 users must install the KB884020 update from Microsoft [61746]

DESCRIPTION On a computer that is running Microsoft Windows XP SP2, programs that connect to IP addresses that are in the loopback address range may not work as expected. For example, you may receive an error message that says that you cannot establish a connection. The OnDemand access agent is in this category: it uses the local loopback address (127.0.0.2) to redirect and secure traffic through the appliance.

SOLUTION Customers should install this patch from the Microsoft site:
<http://support.microsoft.com/kb/884020/>

WorkPlace client provisioning fails with IE7 on Vista because Protected Mode is disabled [62578]

DESCRIPTION If IE7 is launched by right-clicking the IE icon and selecting **Run as administrator**, or if the browser is launched with administrative privileges from another application (which is what happens during client provisioning), **Protected Mode** is disabled. The result is that Aventail Access Manager is successfully installed, but the client is not.

Web proxy service agents fail to activate if Kaspersky Internet security suite is running [62644]

DESCRIPTION On a Vista Ultimate computer using IE7, Aventail agents that use the Web proxy service (which manages HTTP and TCP/IP connects from Web browsers, Aventail OnDemand, and Connect Mobile) fail to activate if the Kaspersky Internet security suite is running. This antivirus program will not allow Aventail .jar files to be installed, resulting in exceptions in the Java Console.

Network shares are not accessible using a virtual IP address [62932]

DESCRIPTION If you run either of the tunnel clients in split tunnel mode (where traffic bound for resources defined in AMC is redirected through the tunnel), you will not have access to network file shares if you are running the Microsoft Vista operating system.

Outlook Web Access Exchange 2003: Not able to type in new mail window [63044]

DESCRIPTION If you are using Windows Internet Explorer 7.0 and Microsoft OWA Exchange 2003 on a client computer running Vista, you may be unable to compose a message.

Release Notes

SOLUTION Refer to the following Microsoft knowledgebase article for instructions on installing a patch on your Microsoft Exchange Server 2003 that addresses this issue:
<http://support.microsoft.com/?kbid=924334>

Outlook Web Access Exchange 2003 & 2007: Cannot attach image files [63087]

DESCRIPTION If you are using Windows Internet Explorer 7.0 and Microsoft OWA Exchange 2003 on a client computer running Vista, you may be unable to attach an image file to a message if your browser is in protected mode.

SOLUTION You have two options to address this issue: either add Outlook Web Access to your list of trusted sites, or turn off protected mode.

Outlook Web Access Exchange 2003: Script error while composing a message [63094]

DESCRIPTION If you are running Internet Explorer 6, you may see the following error message when you compose a message using OWA Exchange 2003:
“A problem with this web page might prevent it from being displayed properly or functioning properly....” This is due to an issue with IE6 that is described in the Microsoft knowledgebase:
<http://support.microsoft.com/default.aspx/kb/929874>

SOLUTION To fix this problem, go to the Microsoft Web site and install the most current cumulative security update for Internet Explorer 6:
<http://www.microsoft.com/technet/security/current.aspx>

IE7 fails to use Translated Web when ActiveX and Java are disabled [63132]

DESCRIPTION If ActiveX and Java are both disabled on a client computer running Vista, the user will see a script error and be unable to access WorkPlace. (Normally, Workplace would revert to Translated Web mode.) This error occurs only if Java is installed, but disabled.

Driver warning dialog box during Connect tunnel installation [63154]

DESCRIPTION On a computer running Vista SP1, a Windows Security alert box appears during installation of Connect tunnel, prompting the user to install the Aventail device software. (This is not an issue in the current release of Vista.)

SOLUTION Users should click **Install** to continue Connect tunnel installation; they will not be reprompted.

In split tunnel mode, file shares are not always redirected to the appliance [63383]

DESCRIPTION In split tunnel mode, traffic bound for resources defined on the appliance is redirected through the tunnel, and all other traffic is routed as normal. With 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 connect 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.

Release Notes

Agent provisioning works only if UAC is disabled [69950]

DESCRIPTION The User Account Control (UAC) feature of the Vista operating system alerts users to security-related conditions. If you are running Vista Ultimate, agent provisioning fails when UAC is disabled.

SOLUTION Install Vista Ultimate SP1.

Access to WorkPlace fails with Java 6 updates 1 through 6 [74025]

DESCRIPTION Access to Aventail WorkPlace fails if the end point device is installed with any of a series of updates to Java 6 from Sun Microsystems: update 1 through 6, inclusive. If one of these updates is installed the appliance can no longer properly detect the Web browser's proxy information. Java 6 update 7 and later works correctly; Java 5 is also supported.

Connect Tunnel

Cannot access the appliance if specified proxy server is unavailable [58785]

DESCRIPTION If Internet Explorer is configured to use an outbound HTTP proxy server, Connect tunnel will attempt 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.

SOLUTION Remove the proxy setting from the browser.

Connect tunnel fails to establish the connection when Sygate Personal Firewall is enabled. [60737]

DESCRIPTION Using Sygate Personal Firewall 5.6 with default settings, Connect tunnel can establish a VPN tunnel, but then closes it with an error message ("The transport connection was aborted by the local system").

SOLUTION Add an "Allow" rule to Sygate Personal Firewall that allows connections to 224.0.0.22 (a multicast address used by IGMP, the Internet Group Multicast Protocol). Once this rule is added, Connect tunnel can successfully establish the tunnel and connections are allowed. You must also configure Sygate Personal Firewall to allow the following processes to access the network when prompted during/after tunnel establishment:

- *explorer.exe*
- *svchost.exe*
- *csrss.exe*
- *ngvpnmgr.exe*

Using dial-up and remote proxy for the connection to the Internet [61056]

DESCRIPTION If you use a dial-up connection to the Internet, and the community to which you are assigned is configured for remote proxy, Internet browsing may not traverse the remote proxy (this applies regardless of whether the remote proxy was configured manually or using a .pac file).

SOLUTION 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.)

Desktop icon for Connect tunnel in WorkPlace not present for all Linux users [61167]

DESCRIPTION When you provision Connect tunnel from WorkPlace and the user downloads and installs the client, an icon is normally created 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.

Release Notes

SOLUTION 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.

Internet is accessible using Firefox in redirect all mode if proxy settings are configured on both IE/Firefox browsers [61605]

DESCRIPTION When configuring the tunnel clients, you must specify a redirection mode, which determines how client traffic is redirected to the appliance. In redirect all mode, traffic is redirected through the tunnel regardless of how resources are defined in AMC. This works in Internet Explorer, which honors the device's Windows Proxy Settings. Mozilla Firefox, on the other hand, ignores the interface-specific proxy settings and just sends all traffic out the proxy server.

Tunnel clients unable to reconnect over an access point that requires authentication [61730]

DESCRIPTION On a Macintosh device, the VPN tunnel cannot be re-established 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.

A realm with international characters must be selected from the Browse Login Groups dialog box [61735]

DESCRIPTION A realm that you create in AMC can be given a name that includes extended ASCII or double-byte characters (for example, "Berliner Bär"). When a user logs in to a WorkPlace realm that includes these characters, and then installs Connect tunnel, he or she will not be able to establish a VPN connection to the realm shown in the Properties dialog box.

SOLUTION Users must follow these steps to work around this issue:

1. Make sure you are not yet connected to the VPN using Connect tunnel.
2. In the Aventail Connect login dialog box, click **Properties**.
3. Click the **General** tab, and then click **Change**. The **Browse Login Groups** dialog box appears and displays the list of login groups.
4. Select the name of the login group (in this case, "Berliner Bär").

Error: "An incompatible version of this product is already installed" [61823]

DESCRIPTION The setup programs for the Connect tunnel and OnDemand tunnel clients do not allow you to install software updates that use different language resources. If a localized release of the tunnel client is installed, for example, a subsequent upgrade to an English-only release will display an error message ("An incompatible version of this product is already installed. Please remove it using Add/Remove Programs in the Windows Control Panel, and then try again").

SOLUTION If you receive this error message while installing a release of one of the tunnel clients, use the Windows **Add/Remove Programs** utility to remove the current client, and then run setup again.

"Redirect all mode" and an internal proxy server [63247]

DESCRIPTION In redirect all mode, appliance traffic is redirected through the VPN tunnel regardless of how resources are defined in AMC. In this mode you can also configure traffic bound for the Internet to be redirected through an internal proxy server when the VPN connection is active.

Windows Connect tunnel traffic that should not be proxied must be explicitly excluded. On the **Network Tunnel Client Settings** page in AMC, type the host names, IP addresses, or domain names of any resources that you do not want redirected through the proxy server.

Release Notes

OnDemand Tunnel

Note: Issue 61823 above applies to both Connect Tunnel and OnDemand Tunnel.

HTTPS traffic routed through proxy in clustered configuration [60871]

DESCRIPTION If a Firefox browser is configured to use an HTTP proxy, OnDemand tunnel (configured in redirect-all mode) incorrectly routes HTTPS traffic through the proxy when the appliance is running in a clustered configuration. When accessing a stand-alone appliance, the client ignores the HTTP proxy setting and properly routes HTTPS traffic based on the proxy settings configured in Firefox.

Script error in WorkPlace when a remote proxy is manually configured for a community [61503]

DESCRIPTION When an Internet Explorer user logs in to WorkPlace and is classified into a community that requires OnDemand tunnel, he or she will encounter a script error if a remote proxy server (for access to the Internet) has been manually configured for that community.

The system tray icon appears when OnDemand Tunnel is running inside ASD [69893]

DESCRIPTION If you create a realm that uses OnDemand as the access method and in which sessions are run within Aventail Secure Desktop (ASD),- the OnDemand icon appears in the system tray; it should not be displayed inside of an ASD session.

OnDemand installation and upgrades must be done in connection with a single appliance [71411]

DESCRIPTION When OnDemand Tunnel is installed for the first time, the installation must be performed by an administrator. A subsequent upgrade can be performed by a non-administrator user, but in the current release it must be upgraded from a single appliance.

Connect Mobile

Trend Micro Mobile Security real-time scanning prevents Connect Mobile installation [60183]

DESCRIPTION Trend Micro Mobile Security performs automatic, real-time scanning and virus detection on handhelds. If real-time scanning is enabled, installing or uninstalling Connect Mobile will fail.

SOLUTION Disable real-time scanning before installing or uninstalling Connect Mobile.

Small form factor devices placed in a Quarantine zone must open a new browser window [60773]

DESCRIPTION If a user logs in to WorkPlace with a small form factor device and his device profile is a match for a Quarantine zone, he cannot log in again by clicking the **Return to login page** button or the Web browser's **Back** button.

SOLUTION To log in again, the user must re-enter the WorkPlace URL in the browser (Pocket Internet Explorer): *https://www.xxx.yyy.zzz/WorkPlace/*. You can also use AMC to place small form factor devices in a different kind of zone (the Default zone, or a Standard or Deny zone) using a device profile.

OnDemand Proxy

OnDemand Proxy must be reinstalled if users upgrade from Vista to Vista SP1 [68628]

DESCRIPTION OnDemand proxy users who upgrade from Vista to Vista SP1 will see an error when they try to access WorkPlace.

Release Notes

SOLUTION OnDemand proxy users who want to upgrade from Vista to Vista SP1 must uninstall their current copy of OnDemand proxy. Uninstalling OnDemand proxy can be done before or after the upgrade to Vista SP1; reinstalling OnDemand should be done after the Vista upgrade.

To activate OnDemand Proxy, cache setting for JVM must be selected [70079, 70080]

DESCRIPTION If both ActiveX and UAC (User Account Control) are disabled on a client computer running Vista SP1, OnDemand Proxy can be installed but fails to activate unless Java is configured to keep a cache of temporary files on the local computer. To change the cache setting, go to Control Panel—>Java—>Temporary Internet Files—>Settings—>Keep temporary files on my computer.

End Point Control

EPC Quarantine zone classification fails after proxy server is specified in Internet Explorer [60939]

DESCRIPTION If you create a community in which the “fallback” option for client devices that do not match any zones is a Quarantine zone, and you then specify a proxy server for outbound access to the Internet in Internet Explorer, subsequent connection requests that should be quarantined will fall through to the Default zone instead.

Device profile specifying a client certificate in the machine store fails for non-privileged user [61578]

DESCRIPTION A Windows device profile can be set up that checks for the presence of a certain client certificate on a user's device in either the machine or user store. However, on an end point device running Windows Vista, the machine store cannot be opened for a user who does not have Windows administrator rights. The search for the client certificate therefore fails and the user is classified into whatever you have configured as the fallback zone (a Quarantine zone or the Default zone).

Zone classification fails on Traditional Chinese OS with AV “PC-cillin 2006” [62045]

DESCRIPTION If you are using a Traditional Chinese version of Windows XP Professional and you have a device profile that specifies the Chinese version of the antivirus program *PC-cillin 2006* from Trend Micro, Inc., zone classification will fail.

Zone classification fails with certificate device profile on Linux and Mac [69625]

DESCRIPTION Import a root certificate to the appliance and create a Standard zone that requires as part of a device's profile on either the Mac OS or Linux platform. Even if the client certificate is imported, the client is relegated to the Default zone rather than the Standard zone you created. The zone classification fails because the appliance is not yet integrated with the certificate store for the operating system or the browser.

Persistent EPC fails if UAC and ActiveX are disabled, even if Java is enabled [70537]

DESCRIPTION Client systems are usually checked for required security features, such as firewall and antivirus software, when users log in. You can now re-check those clients periodically on a per-zone basis. If UAC and ActiveX are disabled persistent EPC fails, even if Java is enabled.

SOLUTION To work around this issue, enable ActiveX

Aventail Cache Control/Aventail Secure Desktop

Incorrect error message is displayed with installation problems on Macintosh [60378]

DESCRIPTION If Aventail Cache Control cannot install to the specified folder on a Macintosh system, it displays the message “ACC is getting downloaded, please wait.”

SOLUTION Ensure that the folder */usr/bin* exists on the Macintosh computer and then try again.

Release Notes

Session-related URL not removed from cache in Safari [60528]

DESCRIPTION When a user logs out of WorkPlace using a Safari Web browser, Aventail Cache Control does not remove the session-related URL from the cache.

SOLUTION Instead of clicking **Log out** in WorkPlace, the user should close the Safari Web browser window in which WorkPlace is running.

Data is cleared when ACC is temporarily disabled [60805]

DESCRIPTION If a user logs in to a realm that requires Aventail Cache Control, accesses a Web site, and then disables cache control manually, all of his Web browser data (URLs, browser history, and cache) is deleted, even the data collected while Aventail Cache Control was disabled.

Inactivity timeout is not honored if the client is placed in standby mode [61247]

DESCRIPTION You can specify a timeout period for the data protection agents (Aventail Cache Control or Aventail Secure Desktop), after which inactive user connections are automatically terminated and data is removed from the client. However, if the client is in standby mode, the inactivity period is not reached and the session remains active.

Citrix ActiveX agent cannot be run together with ASD [61404]

DESCRIPTION In Internet Explorer, the Aventail Secure Desktop blocks the ability to download and execute ActiveX controls. In this case, the Citrix Java applet is used instead, if it has been uploaded through the Aventail Management Console.

Accessing WTS resource terminates ASD [62778]

DESCRIPTION After installing Aventail Access Manager, users who access a graphical terminal shortcut (using Windows Terminal Services) in a realm that requires Aventail Secure Desktop are prompted to accept a Java prompt in a new window. Once they do this, however, ASD terminates and all of the browser windows are closed.

This problem occurs only with new installation of Aventail Access Manager. If a user has accessed the Aventail appliance and installed AAM from a realm that does not require ASD, graphical terminal shortcuts will work as expected.

Microsoft Remote Assistance does not work with ASD [62903]

DESCRIPTION Aventail Secure Desktop is incompatible with Remote Assistance, a Microsoft Windows technology that enables Windows XP users to help each other over the Internet. Users who are running ASD and try to open Remote Assistance will see an error message ("A Program Could not Start").

User inactivity timeout ignored in ASD [63261]

DESCRIPTION In ASD, you can set an inactivity timer that is triggered when no keyboard or mouse activity is detected; when the configured timeout length is reached, the session is ended. This timeout can be set in the ASD Configuration Manager, or the **Configure Community** page in AMC. In v9.0.0, these ASD inactivity settings are ignored.

On Vista OS, closing browser window results in error [65564]

DESCRIPTION When a user logs in to WorkPlace and runs ASD, the OnDemand Proxy access agent is successfully activated. After logging out of WorkPlace, ASD behaves properly, removing the browser's cache and history. But after closing the browser the user sees the follow error message: "Windows Host Process (Rundll 32) has stopped working." You can safely dismiss this message.

Release Notes

Aventail WorkPlace

Unable to access Web resources on Firefox browser with proxy server [60138]

DESCRIPTION Neither OnDemand proxy (in dynamic mode) nor OnDemand tunnel is able to modify proxy settings in Firefox. As a result, Firefox tries to access WorkPlace links directly through its original proxy, which fails because the links are no longer translated.

Certificate authentication process stalls during login to WorkPlace [61269]

DESCRIPTION When you connect to WorkPlace using Internet Explorer on a PDA that is running Windows Mobile 5, and you attempt to log in to a realm that requires a client certificate, the session appears to stall.

SOLUTION Click the **Next** button.

DNS servers that resolve only internal addresses cause login delays [62767]

DESCRIPTION During login, the Aventail appliance does a DNS lookup on IP addresses and subnets to determine whether a hostname matches (for example) an item in an access list rule. If your DNS server is not configured to resolve any external addresses, just internal ones, the login will succeed but can take a couple of minutes.

File upload breaks when file size is beyond 500 Mega Bytes [66196]

DESCRIPTION Unable to upload file more than 250 MB via workplace, despite configuring to upload 1000MB file.

WorkPlace UI has some cosmetic issues with IE6 [69114, 69292]

DESCRIPTION If you log in to WorkPlace using Internet Explorer 6, some UI elements (for example, the buttons that appear in the top-right corner of the page: Log out, Help, Details) are not displayed correctly. The workaround is to use IE7 instead.

Shortcuts using the *XXX_USERNAME_XXX* resource variable do not work correctly in v10.0 [70396]

DESCRIPTION If you have a WorkPlace network shortcut referencing a resource that contains the username variable available in firmware versions prior to v10.0 (for example, `\\example\users\XXX_Username_XXX`), it will not work correctly in v10.0.

SOLUTION To work around this issue, edit the resource definition and replace `XXX_Username_XXX` with the new v10.0 built-in variable for user name (`{Session.userName}`).

AMC Configuration

Searching for user/groups is limited to 1,000 or 1,500 entries [61955]

DESCRIPTION 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) will display no results in AMC.

Browsing AD Tree authentication server groups shows only the members in group's domain [73917]

DESCRIPTION When using a Microsoft Active Directory Tree authentication server to browse for groups, AMC displays only group members (in the lower-right pane) that are in the same domain as the group being browsed. All group members should be displayed, including those in other domains. This will be fixed in the next maintenance release.

Release Notes

User sessions showing incorrect access request details [73936]

DESCRIPTION If you upgrade your appliance and immediately begin using it, the access requests on the **Session Details** page incorrectly indicate that some requests are being denied (for example, the rule summary might read as follows: "Access to this destination has been rejected by an implicit deny all rule at the end of the Access Control list").

SOLUTION To work around this issue, apply at least one other change after you upgrade and the appliance restarts. Applying an additional change in AMC populates the database with policy IDs.

AMC can't find child domains when there is a case mismatch with the root domain name [73963]

DESCRIPTION When you set up a Microsoft Active Directory Tree authentication server, AMC queries the trusted domains to build a list of child domains from the global catalog, showing only those that are at or below the root. The known issue is that AMC does a case-sensitive comparison when it builds this list; if the root domain is corp.honj.com, a child domain of UK.corp.Honj.com will not be included in the AMC list because the domain is not an exact match.

SOLUTION To work around this issue, rename the domain, or use regular AD and the global catalog if you can assume that all usernames are unique across the AD tree. This will be fixed in the next maintenance release.

Fixes Incorporated in This Release

Issues fixed in this release

The following known issues from earlier versions of the appliance are fixed in this release. The numbers refer to internal SonicWALL Aventail tracking IDs.

Platform/Operating System/AMC

63927	Group Policy is not pushed to client PCs through Connect Tunnel
64032	Hotfix link information does not appear when we rollback and reinstall the same hotfix
64294	SNMP trap for the following OID:1.3.6.1.4.1.2021.2 shows that <code>srvcmond</code> is not running
64336	After importing cluster configuration and upgrading to version 8.9 WorkPlace stops responding on a standalone appliance
64437	Unexpected reboot when eth0 broadcast address is pinged from Connect Tunnel client
64856	Custom hostname causes SNMP data query to fail
65408	SharePoint portal breaks when accessed in Translated mode
66062	Large data read causes SSL negotiation; Connect Tunnel times out
66131	Citrix NAM published application does not load
66213	Radius authentication fails the first time after installing <code>clt-hotfix-004</code> and later
66371	Keyboard layout changes when using RDP NAM
66378	When AD authentication server takes too long to respond, failover does not occur for end user
66631	Error message ("Invalid Format Error") while defining a URL resource with a *space* in it
67394	AAM fails if User Account Control (UAC) is disabled
69027	Incorrectly displays Thai characters in extraweb and extranet logging
69078	Ctrl + mouse click doesn't map correctly to right-click with RDP Java NAM (OSX)
69914	Buffer overflow message at INFO level logs
70206	Ability to disable copy/paste in RDP NAMs

Release Notes

- 70258 Log message with incorrect dates appear intermittently in *extranet_access.log*
- 74065 After upgrade, licensing system rejects a license if the auth code is in uppercase,.

Connect Tunnel

- 60251 Macintosh and Linux clients lack support for null authentication
- 60910 Appliance accessible from Connect tunnel even when not explicitly provisioned
- 61666 Certificate selection dialog includes certificates that are not trusted by the appliance
- 64116 Macintosh client installation package in AMC should support OS X 10.5
- 69180 Deploying OnDemand Tunnel using Firefox 2.0 over a proxy may result in errors
- 70004 Can't launch Connect Tunnel on Windows Server 2003 SP1
- 70048 Connect Tunnel installation fails on Vista SP1

Connect Mobile

- 64097 Switching to a different VPN appliance requires rebooting the mobile device

EPC

- 60946 EPC zone classification fails after remediation steps are taken
- 63656 Add Norton Anti-Virus 2008 support for EPC on Vista OS
- 68258 Zone classification for mobile devices fails when using WorkPlace instead of Connect Mobile
- 70611 Zone classification for Mac OS fails if the device profile is looking for a match in a series

Aventail WorkPlace

- 62606 Terminal shortcuts must be launched twice with Macintosh OS X v10.3
- 63643 SSO to Citrix Farm is not working if the user logs in to the workplace using userPrincipleName
- 69109 Firefox 3.0 support is not available
- 69579, 70564 Session details are not always accurate in Workplace
- 70884 Username field populated with root while accessing an RDP resource through workplace

Technical Documentation and the Knowledge Portal

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

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

Last updated: 12/15/2008