Release Notes

Email Security

Dell SonicWALL Email Security 7.3.6 Appliance Release Notes

Contents

System Compatibility

Dell SonicWALL Email Security 7.3.6 is supported on the following Dell SonicWALL Email Security appliances:

- Dell SonicWALL Email Security 200
- Dell SonicWALL Email Security 300
- Dell SonicWALL Email Security 400
- Dell SonicWALL Email Security 500
- Dell SonicWALL Email Security 3300
- Dell SonicWALL Email Security 4300
- Dell SonicWALL Email Security 6000
- Dell SonicWALL Email Security 8000
- Dell SonicWALL Email Security 8300

Enhancements

The following is a list of new enhancements made to features in the Dell SonicWALL Email Security 7.3.6 Firmware release:

- **McAfee Incremental Updates**
  McAfee Incremental Updates significantly reduce the network bandwidth usage.
- **CLI Commands**
  New CLI commands introduced in Email Security 7.3.6 to force NAI updates (*forcemcafeeupdate* and *forcemcafeeupdatecancel*).
- **Network Path Functionality**
  New Network Pat functionality in Email Security 7.3.6 allows MTA to have “SmartHost with Exception” Routing option.
- **SNMP Service**
  SNMP Service has been upgraded with added support to Start, Stop, and Set Community Strings.
- **Self-Signed Certificates Support**
  Email Security 7.3.6 supports downloading Self-Signed Certificates from LDAP Servers over LDAPs.

- **PMTA Upgrade**
  Powerful Mail Transfer Agent (PMTA) is upgraded to version 4.0r2sb1 in Email Security 7.3.6.
- **Tomcat Upgrade**
  Tomcat is upgraded to version 6.0.35 in Email Security 7.3.6.
- **JRE Upgrade**
  Java Runtime Environment (JRE) is upgraded to version 1.6.0.30 in Email Security 7.3.6.
- **OpenSSL Upgrade**
  OpenSSL is upgraded to version 1.0.0e in Email Security 7.3.6.

Restrictions and Limitations

These are the restrictions and limitations currently reported in the Dell SonicWALL Email Security 7.3.6 Appliance release:

	Symptom	Condition
95936	Auditing and Junk Box messages do not display after downgrading from Dell SonicWALL Email Security 7.3.5 to 7.2.4.	Occurs after a successful upload of the Dell SonicWALL Email Security 7.2.4 Der-signed patch. Upon logging into the appliance again, the user will receive a warning message, as well as no inbound messages in the Auditing and Junk Box screens. **Workaround:** Login to the SNWLCLI and run the 'rebuildsearchdb' command. All messages will be displayed in the Junkbox/Auditing UI.
94121	Virtual IP information does not display on the User Interface after configuring in DHCP mode.	Occurs after attempting to configure the Virtual IPs to eth0 and eth1 from the CLI, using the following commands: vip --add IPADDRESS1 –netmask SUBNETMASK1 –interface eth0 vip --add IPADDRESS2 –netmask SUBNETMASK2 –interface eth1 Upon logging into the User Interface, the existing Virtual IPs do not display. Users are unable to add or delete either Static or DHCP Virtual IPs configured to eth0 or eth1. Virtual IPs are supported for Static Ethernet Addresses ONLY.

Known Issues

These are the known issues currently reported in the Dell SonicWALL Email Security 7.3.6 Appliance release:

	Symptom	Condition
95679	The LCD screen of Dell SonicWALL Email Security 8300 appliances incorrectly displays eth1's IP address and subnet mask for eth0's IP address and subnet mask.	Occurs after enabling or disabling the Ethernet1 port of a Dell SonicWALL Email Security 8300 appliance. When attempting to view the default IP address and subnet mask for the eth0 interface, the LCD displays eth1's IP address and subnet mask, respectively.
95227	The Scheduled Backup process does not confirm the available disk space before initiating a backup zip file creation.	Occurs when attempting to schedule a backup. The Scheduled Backup process should estimate the space required for the backup before initializing a backup zip file creation.
93315	User cannot access appliance if Samba directory is deleted from NAS or SAN.	Occurs when creating a Samba share, then deleting the share from the NAS or SAN. When attempting to login to the appliance, the appliance is unable to be accessed. **Workaround**: Unmount the drive from the Web UI before deleting.

Resolved Known Issues

These are the resolved known issues currently reported in the Dell SonicWALL Email Security 7.3.6 Appliance release:

	Symptom	Condition
112222 **120042**	Web UI cross-site scripting vulnerability found in Email Security 7.3.5 or earlier release builds.	The vulnerability may be exposed when attempting to access some of the Email Security administrative configuration pages using administrative credentials. To exploit this vulnerability, the attacker must have access to the web UI, which is typically only available on the local LAN. In addition, the attacker must have administrative credentials. The pages impacted are only accessible to the administrator, so it does not pose any risk to normal users accessing the web UI. The vulnerability also does not specifically target or impact message processing, anti-spam, anti-virus or policy and compliance protection. For these reasons the risk is considered low.
111245	The TLS implementation of the SMTP Proxy defaults to a large set of ciphers, including weak ciphers that are required by modern security compliance tests to be disabled.	The client side TLS request demanded the use of a weak cipher. Email Security always returns the strongest cipher that the client supports.
110710	The Flood Protection threshold is not being triggered by secondary aliases.	Occurs when flood sender sends more emails than the value specified in message threshold by the administrator. Flood protection threshold is not accounting for email aliases associated with the primary address.

110460	Customers with larger user lists and multiple RAs may get 'User Map is Stale' alerts.	Occurs when using large user maps in a split mode setup with multiple RAs. This may issue stale alerts because of an issue with replicating the data in a timely manner.
109769	The CA Certificate keystore in the Java Directory is empty with no certificates imported inside. LDAPs are also unable to work correctly because of dependence on the certificates.	Occurs when downloading certificates into the JRE directory. New certificates are not getting added to the CA Certs file in JRE directory.
109027	Tomcat allows the use of weak SSL ciphers, which is a potential security risk and does not comply with modern security compliance tests (PCI).	Occurs when conducting a PCI compliance scan on the Email Security system. The results show that the Email Security system does not comply with PCI standards.
108993	MTA routing needs a "SmartHost with Exceptions" routing option, where the exception domains use MX record routing.	Occurs when selecting MTA routing options for routing email using SmartHost to the destination server.
108152	The DSN template file path no longer displays in the PMTA config.dat after new changes are made to the MTA.	Occurs when new changes are made to the MTA. As a result, the MTA stops, and does not restart. **Workaround:** Add the DSN template file path manually in the PMTA configuration file.
100550	MTA services do not start and an error message displays in the config.dat file.	Occurs if the data directory is a UNC network path with spaces. The MTA does not start.
87748	The View button in the Junk Summary are not working for alias addresses, yet work fine for primary addresses. This is only seen when users are Global or non-LDAP users.	Occurs when clicking the View button for junk messages in the Junk Summary. The primary addresses that have aliases receiving junk for the aliases are unable to use the View button on the Junk Summary that was sent to the primary address. **Workaround:** Configure an LDAP server that returns no users. This creates the multi_ldap.xml with the necessary structure. You can also drop an empty multi_ldap.xml under $DATADIR$\. However, if you do this and decide to add an LDAP, this empty file will first have to be manually deleted.

Important Note for McAfee Anti-Virus Subscribers

Feature	Summary
Upgrade McAfee to Engine 5400	McAfee will be ending support for the anti-virus scan engine v5300 (running in Dell SonicWALL Email Security versions 7.1.2 and lower). Dell SonicWALL Email security customers using McAfee antivirus will need to upgrade their email security firmware by February 28th, 2010.

Dell SonicWALL strongly recommends customers running McAfee to upgrade to the latest 7.3.6 firmware version.

McAfee has released an upgraded version of their anti-virus engine using a newer, enhanced format that provides smaller, faster signature updates, improved bandwidth, and better detection of the latest malware. As of **February 28, 2010**, Dell SonicWALL McAfee anti-virus engines in the firmware versions 7.1.2 and lower will no longer receive

virus signature updates. Customers using McAfee anti-virus will begin to see degraded virus protection and will no longer be protected against the latest virus outbreaks.

Customers can simply upgrade their Dell SonicWALL Email Security firmware to receive the benefits of the McAfee upgrade. The impact will be largely transparent to administrators and end customers. To ease the transition, Dell SonicWALL will offer customers the following upgrade path:

- Upgrade to Dell SonicWALL's newest, latest firmware (version 7.3.6). In addition to the enhanced Dell SonicWALL McAfee engine, firmware version 7.3.6 offers several significant enhancements, including best-in-class effectiveness, bandwidth improvement, improved ease of management and significant scalability improvements.

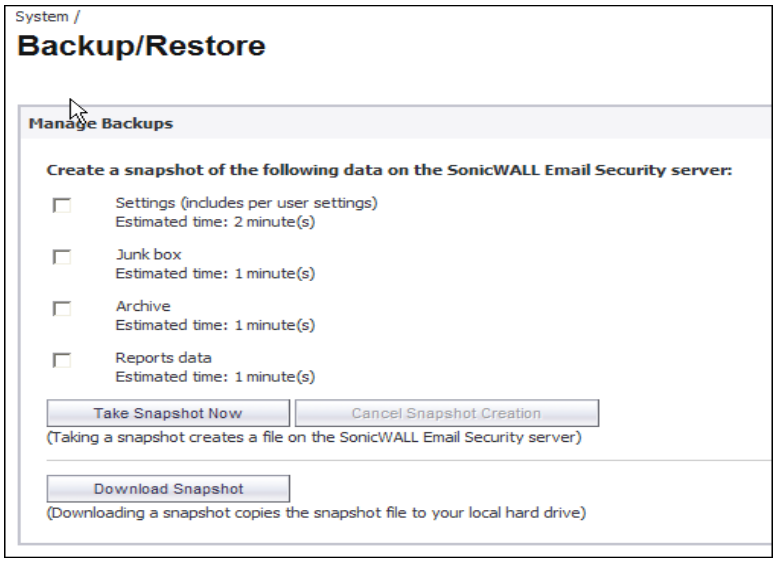
Upgrading the Email Security Firmware

The following procedures are for upgrading an existing Email Security appliance.

Backing Up Your Existing Environment

Before you upgrade your firmware, you should back up your existing environment. This will enable you to restore it if you decide to change back for some reason. Your backup should include the settings files, including the per user settings. To back up your existing environment:

1. Login to Email Security interface using the **admin** account
2. In the left navigation pane under **System**, choose **Backup/Restore**. You will see the Backup/Restore page:

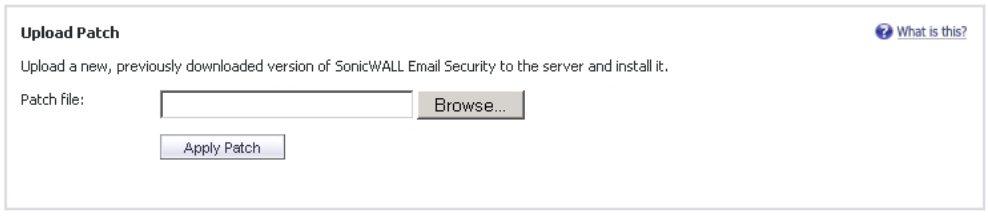


3. In the Manage Backups section, select **Settings**.
4. Click **Take Snapshot Now** to create a snapshot.
5. Click **Download Snapshot** to save the snapshot to your local file system

Upgrading Your Dell SonicWALL Email Security Firmware

Follow this procedure to upgrade your existing Email Security firmware.

1. Navigate to the System > Advanced page and scroll down to the **Upload Patch** section.



2. Click **Browse** to locate the Email Security Firmware file on your local file system, and then click **Apply Patch**.
3. As part of the upgrade process, the Email Security appliance will reboot. The upgrade process could take between 10-20 minutes. All the settings and data will be preserved.

NOTE for ES8300

Your ES8300 is equipped with a battery backup unit on the RAID Controller Card, which allows the appliance to write volatile memory to disk in the event of a loss of power. This battery backup unit must be charged for 24 hours. When deploying your ES8300 appliance, follow the startup and registration instructions detailed in the Getting Started Guide, and then allow the battery backup in the unit to charge for 24 hours. If the battery is not fully charged, some RAID features are turned off, and the appliance performance is temporarily impaired until the battery is fully charged.

Related Technical Documentation

For basic and advanced deployment examples, Dell SonicWALL documentation is available in the Dell SonicWALL Technical Documentation Online Library:

http://www.sonicwall.com/us/Support.html

Also, refer to the following related Knowledge Based articles:

How to Upgrade a Windows server in Split Mode Configuration

https://www.fuzeqna.com/sonicwallkb/consumer/kbdetail.asp?kbid=4891

How to Setup/Breakup Cluster Licensing for Email Security's Split-Configuration

https://www.fuzeqna.com/sonicwallkb/consumer/kbdetail.asp?kbid=5244

How to Recover a Non-Accessible Email Security Appliance

https://www.fuzeqna.com/sonicwallkb/consumer/kbdetail.asp?kbid=8486

How to Reset the Authentication for GUI Login Back to Default Credentials

https://www.fuzeqna.com/sonicwallkb/consumer/kbdetail.asp?kbid=5207

_____

Last updated: 9/20/2012