Dell SonicWALL™ E-Class SRA / Secure Mobile Access 10.7.2

Release Notes

May, 2015

These release notes provide information about the Dell SonicWALL™ E-Class SRA / Secure Mobile Access (SMA) 10.7.2 release.

About Dell SonicWALL E-Class SRA / SMA 10.7.2

Dell SonicWALL E-Class SRA / SMA 10.7.2 is the Initial Release for Dell Secure Mobile Access 6200 and 7200 appliances.

- SMA 6200
- SMA 7200

This release also resolves a number of issues found in previous releases. See the Resolved issues section for more information.

Supported platforms

The Dell SonicWALL E-Class SRA / SMA 10.7.2 release is supported on the following E-Class SRA and Secure Mobile Access appliances:

- EX9000
- EX7000
- EX6000
- E-Class SRA Virtual Appliance
- SMA 7200
- SMA 6200
- SMA Virtual Appliance

Client machines running version 10.7.2 client software should be used with E-Class SRA or SMA appliances running one of the following versions:

- Secure Mobile Access 11.2, 11.1, 11.0
- E-Class SRA 10.7.2, 10.7.1, 10.7.0
- E-Class SRA 10.6.5

NOTE: Windows 10 is not supported for client machines in this release.

NOTE: Secure Virtual Desktop is not supported on client machines running Windows 8 or 8.1. This is a known issue with ID 137483.

Resolved issues

The following is a list of issues addressed in this release.

AMC resolved issues

Resolved issue	Issue ID
Exporting the unregistered device log to XML fails and AMC logs show the error, “Caught exception while trying to validate BASIC credentials for device export: java.lang.NullPointerException”. Occurs when a custom user exists, such as a local admin user, while attempting to export the list of unregistered devices to an XML format.	155313
Agent configuration for Connect Tunnel custom results in errors about the zip file, including “The zip archive does not contain the following directories: {0}”. Occurs when the DefaultBranding.zip file is downloaded from AMC, modified by adding the custom files, re-zipped including directories and modified images, and then imported to AMC.	145057
AMC configuration becomes corrupted when a new realm with default settings is created after deleting all other realms along with their related resources, users and groups, and access control lists. Occurs when one of the deleted realms had a community in it that referenced a tunnel SNAT pool which became orphaned after deleting the realm.	143715

Vulnerability resolved issues

Resolved issue	Issue ID
A vulnerability in the mdnsd code package included in WorkPlace can allow responses to mDNS unicast queries from the WAN with information about the product. Occurs when incoming and outgoing mDNS messages and advertisements are allowed on the external interface (X1) during initial appliance setup and afterwards.	157380
A vulnerability (CVE-2014-0114) in the Apache Struts package included in WorkPlace can allow unauthorized disclosure of information, modification, or disruption of service. AMC includes Struts, but is not vulnerable due to other factors. Occurs when an attacker sends an URL request that includes a “class” parameter.	145940

Known issues

The following is a list of known issues in this release.

Authentication known issues

Known issue	Issue ID
Certificate-based authentication fails and results in a “page cannot be displayed” error. Occurs when both the TLS 1.2 and SSLv2 protocols are enabled in an Internet Explorer browser on Windows 7 and higher.	151224

Cache Cleaner known issues

Known issue	Issue ID
CacheCleaner 1.3.20.1 fails to clear password, history, typed addresses, cache, cookies, download history, and form data. Occurs when using Firefox browser version 34.	155239

Connect Tunnel known issues

Known issue	Issue ID
Downloading Connect Tunnel from the appliance copies unnecessary files to the client system, displays a warning with the message "Do you want to copy this folder without encryption?" and fails to change the desktop CT icon as expected. Occurs when the administrator has configured Connect Tunnel to have custom branding.	149983

End Point Control known issues

Known issue	Issue ID
A Cache Cleaner wipe message is shown upon logging out from WorkPlace. Occurs when a user logs out of a realm in which Secure Virtual Desktop is enabled for the zone, but is not enabled for End Point Control agents.	140145

ExtraWeb Proxy known issues

Known issue	Issue ID
Proxy clients including OnDemand Proxy, ExtraWeb Proxy (EWPCA), and OnDemand Tunnel are disconnected from the appliance immediately after the user enters valid credentials at the EW login prompt. Occurs when a manual outbound proxy is configured at system level on the appliance, and then a user connects to the appliance from any browser on a Windows client machine.	156419

Provisioning known issues

Known issue	Issue ID
Connect Tunnel and OnDemand Tunnel clients fail to connect to the appliance. Occurs when the client computer is running the Windows 10 preview release. **Workaround:** For Connect Tunnel to work, restart the client computer after installing Connect Tunnel.	157214
Agent provisioning fails. Occurs when using MAC 10.9 X64 with and Safari 7 and Java 7.25 or 7.40. **Workaround:** Mac OS 10.9 users should configure Safari to ignore security restrictions by selecting Preferences > Security > Manage Website Settings > Java 7.25 > Allow (no security restrictions). If using Java 7.40, configure Safari by selecting Preferences > Security > Manage Website Settings > Java 7.40 > Allow and Run in Unsafe Mode.	131895
WorkPlace cannot connect to an ODT/ODP/EWPCA realm. Occurs when an outbound proxy is configured and attempting to connect from a 32-bit or 62-bit client machine running Windows 8, using Internet Explorer 10 or Firefox.	123408

Secure Virtual Desktop known issues

Known issue	Issue ID
A browser does not launch from inside Secure Virtual Desktop. Occurs when using an SVD-enabled realm with Windows 8 or 8.1 and Internet Explorer 10 or 11.	137483

Upgrading known issues

Known issue	Issue ID
Upgrading to SMA 11.1.0 is not supported for SMA 6200 and SMA 7200 appliances. Occurs when trying to upgrade the SMA 6200 or 7200 from 10.7.2 to 11.1.0.	156024
Upgrading Connect Tunnel or OnDemand Tunnel to 10.7.2 from WorkPlace or in client software fails. Occurs when attempting to upgrade tunnel clients from 10.5.x, 10.6.x and previous 10.7.x versions, due to a change in the certificate from SonicWALL Inc. to SonicWALL L.L.C. **Workaround:** Install the tunnel clients from an appliance running 10.6.5 plus Clt-hotfix-10.6.5-353 or higher, or from an appliance running 10.7.1 plus Clt-hotfix-10.7.1-471 or higher, and then upgrade the client to the 10.7.2 version.	157400

WorkPlace known issues

Known issue	Issue ID
WorkPlace access fails with the message, “Unable to authorize request. Zone classification process has not completed.” Occurs when attempting to access WorkPlace using Firefox on a client machine running Ubuntu Linux with Java 1.7u71 is installed. This problem is caused by an issue in Java, see https://bugs.openjdk.java.net/browse/JDK-8064677.	156968
Single Sign-On does not work with a web form in an application accessed via WorkPlace. Occurs when the server sends a dynamic value generated at runtime as part of the HTML page and expects the corresponding name/value pair in the POST request.	135802

Upgrading information

For information about upgrading an E-Class SRA appliance to version 10.7.2 from an earlier release, be sure to consult the *E-Class SRA 10.7.2 Upgrade Guide*, available on https://www.mysonicwall.com or on the Support website at: https://support.software.dell.com/sonicwall-e-class-sra-series/release-notes-guides.

For Tunnel Client upgrade recommendations, see the knowledge base article at: https://support.software.dell.com/kb/sw13783.

Product licensing

Dell SonicWALL E-Class SRA appliances must be registered on MySonicWALL to enable full functionality and the benefits of Dell SonicWALL security services, firmware updates, and technical support.

Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions.

Dell SonicWALL Administration Guides and related documents are available on the Dell Software Support site at https://support.software.dell.com/release-notes-product-select.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the portal provides direct access to product support engineers through an online Service Request system. To access the Support Portal, go to http://software.dell.com/support/.

The site enables you to:

- Create, update, and manage Service Requests (cases)
- View Knowledge Base articles

  https://support.software.dell.com/kb-product-select
- Obtain product notifications
- View instructional videos

  https://support.software.dell.com/videos-product-select
- Engage in community discussions
- Chat with a support engineer

About Dell

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.software.dell.com.

Contacting Dell

Technical support:
Online support

Product questions and sales:
(800) 306-9329

Email:
info@software.dell.com

Patents

For more information about applicable patents, go to http://software.dell.com/legal/patents.aspx.

Trademarks

Dell, the Dell logo, SonicWALL, and Aventail are trademarks of Dell Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others.

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

IMPORTANT NOTE, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Last updated: 5/5/2015

232-002801-00 Rev D