Dell™ Secure Mobile Access 12.0.0

Release Notes

November 2016

These release notes provide information about the Dell Secure Mobile Access (SMA) 12.0.0 release.

About Dell Secure Mobile Access 12.0.0

The Dell Secure Mobile Access (SMA) 12.0.0 release is an early release that provides new features and resolves a number of issues found in previous releases.

Supported platforms

Supported appliances

The Dell SMA 12.0.0 release is supported on the following Dell SMA 1000 series appliances:

- EX9000
- EX7000
- EX6000
- SMA 6200
- SMA 7200
- SMA 8200v (ESX/Hyper-V)

Supported releases

Client machines running version 12.0.0 client software can be used with Dell SMA appliances running one of the following firmware versions:

- 11.4.0
- 10.7.2

New features

Dell Secure Mobile Access (SMA) 12.0 includes the following new features:

- **Central Management Service (CMS) with Global Traffic Optimizer (GTO**) presents a collection of SMA appliances to end users through a single GTO service name (for example access.example.com), which allows users to access their organization's network through an appropriate SMA appliance depending on their global location and other factors.
- **Global Traffic Optimizer (GTO**) supports backend resources such as WorkPlace sites, custom FQDNs, Active-Sync, and Outlook Anywhere, across all appliances in the GTO service, and you can access those resources through the appliances that are part of the GTO service.
- **Biometric Identity Verification** provides the option to use biometric identification to unlock cached credentials on Mobile Connect devices.
- **RDP, VNC, SSH, and Telnet using HTML5** enables clients to connect to backend systems using RDP, VNC, SSH, and Telnet. HTML5 clients can use Single Sign-On (SSO), copy and paste, multiple language keyboard support, scroll back, and dynamic window resizing. Users also have wider connectivity, such as cross-browser, cross-OS support.
- **Legacy and SAML SSO Support with CAM** provides unified Single Sign-On (SSO) support for legacy and SAML federated Software as a Service (SaaS) applications using Cloud Access Manager (CAM) as an Identity Provider (IDP).
- **Central Reports and Analysis (CRA)** feature allows you to view a near real time analysis of what is happening on the CMS managed appliances. You can examine summary information for the entire CMS cluster via charts and graphs on the Central Management Console (CMC).
- **Appliance Management Console (AMC)** and **WorkPlace** management interfaces have a new skin and provide a redesigned page layout**.**
- **GTO with Global High Availability (HA)** is a new solution for SMA 12.0 that facilitates high availability and disaster recovery for SMA products. The High Availability (HA) Pair product is no longer supported as of SMA 12.0.

Deprecated Features

The following features have been deprecated in SMA 12.0:

- GMS
- Secure Sockets Layer (SSL) Version 3.0
- Virtual Assist
- Replication
- High Availability Pair
- Virtual Host with IP Address

Resolved issues

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

Authentication

Resolved issue	Issue ID
Remote authenticated users can access unauthorized areas on the server. Occurs when remote users are logged into the authentication server.	176101

Connect Tunnel

Resolved issue	Issue ID
Connect Tunnel clients get “Modem Not found” error. Occurs when the client tries to launch a VPN client using a USB based Phone Data card connected to a Windows 8.1 Machine.	167997

Firmware

Resolved issue	Issue ID
Appliance firmware does not get upgraded. Occurs when trying to upgrade clients from 10.7.2 to 11.3.	171987
Appliance services will not start. Occurs when attempting to upgrade the firmware from 10.7.2 to 11.3.0 or to 11.4.0.	178267
Group affinity Check for Realms does not get migrated. Occurs when using two authentication servers with Radius as the primary server and attempting to upgrade the firmware from 10.7.2 to 11.4.	178328

Licensing

Resolved issue	Issue ID
The Manage Licenses page shows licenses as Unknown when they should show the company name of the license. Occurs when importing licenses in AMC from mySonicWALL.	178686

Logging

Resolved issue	Issue ID
No audit log is logged when it is expected. Occurs when trying to generate a certificate signing request.	176859
Extraweb displays WorkPlace password in plaintext. Occurs when viewing logs in Extraweb in WorkPlace.	169999

Policy Server

Resolved issue	Issue ID
EX6000 and virtual appliance have memory depletion. Occurs when running appliances in a cluster.	178754
AMC shows Policy Corruption error. Occurs when there are more than 17 configuration backups.	177591

Known issues

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

Central Management

Known issue	Issue ID
The CMS overwrites authentication settings on the SMA appliance during policy synchronization. Occurs when Central User Licensing is disabled at the CMS, and "Each node has its own authentication server" is enabled.	178437
The critical and warning alerts for the event “Permanent/Temporary communication loss” on managed appliances have the same default values. As a result, only the warning alert is raised and the critical alert is NEVER raised. This prevents an SNMP trap from being raised by the CMS. Occurs when one of the managed appliances is rebooted or when the Eth0 interface is shutdown and an alert is generated.	177622
Managed appliances cannot be upgraded from the CMS. Occurs when trying to upgrade managed appliances from 11.4 to 12.0.	177593
FQDN resources cannot be disabled from the Central Management Service (CMS). Occurs when using web applications such as Jira and Confluence with Central Management Service (CMS) with Global Traffic Management (GTO).	177152

Connect Tunnel

Known issue	Issue ID
Connect Tunnel Service (CTS) cannot establish a tunnel. Occurs when "Device Authorization" is configured, and CTS is started.	178422

HTML5 Clients

Known issue	Issue ID
Text cannot be copied and pasted to or from remote computers. Occurs when using the HTML5 clients in the Chrome, Edge, or Firefox browsers.	177501

Virtual Appliance

Known issue	Issue ID
The ESXI virtual appliance cannot be upgraded. Occurs when trying to upgrade an ESXI virtual appliance from 10.7.2 to 12.0 directly.	176950

WorkPlace

Known issue	Issue ID
The French (Belgium) keyboard replaces the English (United states) keyboard and vice versa. Occurs when trying to select the English or French keyboards in WorkPlace.	177333
SSH and Telnet HTML5 clients display an error message. Occurs when trying to use SSH or Telnet in Windows IE10.	178045

Upgrading information

For information about an E-Class SMA appliance to version 12.0.0 from an earlier release, be sure to consult the *Dell SMA 12.0.0 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.

Product licensing

Dell SMA or E-Class SMA 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)
- Obtain product notifications
- Engage in community discussions
- View Knowledge Base articles at:

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

  https://support.software.dell.com/videos-product-select
- Select the version of Mobile Connect that applies to your device at:

  https://support.software.dell.com/sonicwall-mobile-connect/release-notes-guides

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

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: 10/25/2016

232-003397-00 Rev A