Release Notes

Secure Mobile Access | **Dell Secure Mobile Access 11.1.0 Release Notes**

Contents

Release Purpose

Dell Secure Mobile Access 11.1 is a Feature Release with support for Per-App VPN as well as Application Access Control, which was introduced in Dell Secure Mobile Access 11.0. Other new features in 11.1 include CAPTCHA, HTML5, and Dell vWorkSpace Native Access Module support.

At this time, Dell Secure Mobile Access is a new product line intended for use with mobile proof-of-concept and pilot projects. It is not appropriate as an upgrade/migration path for existing E-Class Secure Remote Access (E-Class SRA) installations.

Platform Compatibility

The Dell Secure Mobile Access 11.1.0 release is supported on the following Dell appliances:

- EX9000
- EX7000
- EX6000
- E-Class SRA Virtual Appliance

Note: Windows machines running version 11.1.0 clients should be used with E-Class SRA appliances running one of the following versions:

- 11.1.0
- 11.0.0
- 10.7.1
- 10.6.4

If you are upgrading an E-Class SRA appliance to version 11.1.0 from an earlier release, be sure to consult the upgrade instructions in the *Dell Secure Mobile Access Upgrade Guide* for detailed information. You'll find a copy of this document on the MySonicWALL Web site (www.mysonicwall.com).

What's New in This Release?

This section describes the new or enhanced features included in Secure Mobile Access 11.1.0.

CAPTCHA Support

CAPTCHA (Completely Automated Public Turing Test To Tell Computers and Humans Apart) is effective in preventing the following types of non-human (programmatic) attacks on password systems:

- A bot that attempts to logon by guessing the username/password by iterating through a dictionary of password possibilities.
- A denial-of-service attack from a bot that attempts to lockout users' accounts by forcing a sequence of unsuccessful logons.

The administrator can enable or disable CAPTCHA for a Realm from the AMC console. CAPTCHA is not enabled by default upon installation. When CAPTCHA is enabled for a Realm, the user is not allowed to authenticate unless he/she solves the CAPTCHA challenge. The user can choose to view a different CAPTCHA image if he/she finds the image hard to discern.

HTML5 Support

Secure Mobile Access 11.1.0 supports HTML5 based RDP. This allows RDP access directly from HTML5 compliant browsers and realizes a true clientless RDP with no Java/ActiveX/Flash plugin required. With no dependency on any client, users can connect from any source (Windows, Mac OS, Linux, tablets running iOS or Android) to most Windows systems (desktop, servers, terminal services) and Linux based systems.

Integration with Dell vWorkspace as a Native Access Module

In SMA 11.1.0, Dell vWorkspace is supported as a WorkPlace NAM. This adds to previous WorkPlace NAM support for products and protocols from different vendors like Citrix and VMware. Dell vWorkspace is very similar to the Citrix/XenApp Web Interface. The end user logs into a web portal, authenticates, is presented a list of published applications or desktops, clicks on an icon (an ActiveX/Java applet is downloaded), and then a connection is made to a back-end server.

Support for Apple MDM Per-App VPN Policies

In the current iOS versions, Apple does not allow BYOD per-app VPN policy configurations, such as those in SMA Application Access Control, to be enforced on Apple devices unless it is performed by a Mobile Device Management (MDM) provider. SMA 11.1.0 supports additional requirements to make Application Access Control work in an MDM setting with per-app VPN, specifically with AirWatch. Three levels of access are supported:

1. Device Zone: Application Limits are handled only by the MDM device.
2. App Zone (allow any version): Only applications configured in both the MDM and E-Class SRA appliance are granted access. Access can be controlled and tracked from specific applications to specific network destinations by the E-Class SRA appliance.
3. App Zone (version matching): All of #2, and additionally verify each flow such that the hash of the application matches what is configured on the E-Class SRA appliance. A different version or compromised application is not granted access to the network by the E-Class SRA appliance.

Known Issues

This section contains a list of known issues in Secure Mobile Access 11.1.0.

Authentication

Symptom	Condition / Workaround	Issue
Workplace access is denied with group authorization “MATCH_FALSE” without parsing a subsequent Access Control List (ACL) which permits access.	Occurs when both a local authentication server and an Active Directory or RADIUS authentication server are configured. A local user group contains local users, and an ACL is configured to deny access to resources for that group. A realm uses the AD or RADIUS auth server, and the local auth server is assigned for group affinity checking (authorization) to this realm. Logging in with a user present in the AD or RADIUS server, but not in the local auth server, results in successful authentication, but WorkPlace access is denied due to the configured ACL. This is because the user does not exist in the authorization server during group affinity checking, and the local group is not associated with any realm, causing the ACL rules to be applied to any realm to which the user logs in.	147769

Cache Cleaner

Symptom	Condition / Workaround	Issue
All browsing history items are cleared although the "Clean Session items only" option is enabled.	Occurs when the user logs out from WorkPlace on a realm with Cache Cleaner enabled, using Firefox 25 and higher or Internet Explorer 9, 10, or 11.	147439
Some Cache Cleaner features do not work correctly.	Occurs when using Firefox 29.x and above, or Chrome 34.x and above because OESIS does not support these browser versions. This is applicable on all platforms where cache cleaner is supported.	146301

End Point Control

Symptom	Condition / Workaround	Issue
On Ubuntu 14 (Linux), access to WorkPlace is denied with basic EPC enabled.	Occurs when Device Authorization is enabled and Zone classification fails with equipment ID as basic EPC.	149361

Symptom	Condition / Workaround	Issue
Mac OS X standard users see an Access Denied message after authenticating in WorkPlace.	Occurs when EPC is enabled on the appliance and a non-administrator Mac OS X user logs into WorkPlace using a realm with a community that has a device profile configured for Mac OS X. Observed with Mac OS X 10.7.5, 10.8.5 or 10.9.3 using Safari 7.0.4 or 6.1.4 with Java 7 update 60. **Workaround**: Before logging in, configure Safari to run Java in Unsafe Mode (Safari > Preferences > Security > Manage Website Settings > Java 7.x > Select "Allow Always" and "Run in Unsafe Mode").	146989
The inactivity timeout does not occur if EPC is disabled.	Occurs when EPC is disabled for Extraweb and tunnel clients. In SMA 11.x, the inactivity timeout setting is moved to the zone configuration. In releases prior to 11.0.0, the inactivity timeout was set in the Community > EPC Restrictions page and it would work even with EPC disabled across Extraweb and tunnel clients.	146451

Extraweb

Symptom	Condition / Workaround	Issue
The Outlook Web Access (OWA) page is not displayed in some cases.	Occurs when OWA 2013 is configured as a Port Mapped resource, a Single Sign-On profile is configured under Web services specific to the OWA 2013 resource, and a user attempts to access OWA via WorkPlace using Firefox or Chrome. **Workaround**: Use Internet Explorer 10 or 11, or configure OWA as a Host Mapped resource.	148161
ActiveSync connections from smartphones result in “401 unauthorized” errors, although credentials are correct and working for email access via the web.	Occurs when trying to set up the ActiveSync connection on an Android phone or iPhone, and CAPTCHA is enabled in the realm which is tied to the ActiveSync resource.	147375
The startup page is removed from the URL during redirection. Once valid credentials are entered, instead of displaying the configured startup page the browser displays the WorkPlace for a port-mapped resource or the default page of the backend server for a host-mapped resource.	Occurs when a host-mapped or port-mapped resource is accessed with Linux on Firefox 29 and Java update 55/60. **Workaround**: Access the resource using a custom port instead of custom FQDN in Linux with Firefox 29 and Java 7 update 55/60.	147043
Single Sign-On (SSO) does not work as expected for port mapped resources for both Outlook Web Access (OWA) 2010 and 2013. It only works for the version whose SSO profile was created last in AMC. When accessing the URL resource for the first one, it prompts again for credentials.	Occurs when an SSO profile is created in AMC for Port Mapped OWA <version X> and then a second SSO profile is created in AMC for Port Mapped OWA <version Y>. The cookie that was created for the first SSO profile is overwritten when the second profile is created.	146331

Provisioning

Symptom	Condition / Workaround	Issue
Incorrect icons are displayed after installing agents on the client machine.	Occurs when the SMA 11.x agents (SEM, CT, Webifiers, OPSWAT EPC, possibly others) are installed on the client machine and later uninstalled, then older agents such as those from 10.7.1 are installed on the same machine. The 11.x icons are still displayed for the 10.7.1 agents in Add/Remove Programs and as the CT desktop shortcut.	146205

Virtual Appliance

Symptom	Condition / Workaround	Issue
Support is limited for older versions of ESX.	Occurs when using VMware ESX 4.1. VMware announced that ESX 4.1 is no longer supported as of 5/21/2014.	146795

Windows

Symptom	Condition / Workaround	Issue
Some Secure Mobile Access 11.0.0 features (including client components) do not work on older Windows systems.	Occurs when Secure Mobile Access 11.1.0 and client components are installed on an XP or Vista device (includes SEM and Connect Tunnel). **Note**: Beginning in SMA 11.1, Windows XP is no longer supported and Vista is supported on a best-effort basis only.	146481

WorkPlace

Symptom	Condition / Workaround	Issue
After a successful WorkPlace session, the WorkPlace Details page shows Aventail Access Manager 11.x instead of Secure Endpoint Manager 11.x.	Occurs after installing the SMA 11.x Secure Endpoint Manager and establishing a successful 11.x WorkPlace session from the client machine, and then disconnecting that WorkPlace session and connecting to a 10.7.1 appliance based WorkPlace session and installing Aventail Access Manager 10.7.1.	146948

Resolved Issues

This section contains a list of issues in previous versions that were resolved in the Secure Mobile Access 11.1.0 release.

End Point Control

Symptom	Condition / Workaround	Issue
The user is unexpectedly prompted to install the Secure Endpoint Manager after logging in to a Community with only web access.	Occurs when the global Enable End Point Control checkbox is selected and the Community is configured for web-only use with either a Translated or Host Mapped URL Resource with no End Point Control (EPC) zone in use. SEM should not be required in this case.	148741

ExtraWeb

Symptom	Condition / Workaround	Issue
The list of programs in Windows Add/Remove on the client machine shows the installed OnDemand proxy agent as "Dell SMA Web Proxy agent" instead of "Dell SMA OnDemand Proxy agent".	Occurs when the OnDemand Proxy agent is enabled as an Access Method for a community, and a Windows client machine connects to WorkPlace and installs all client components.	146944

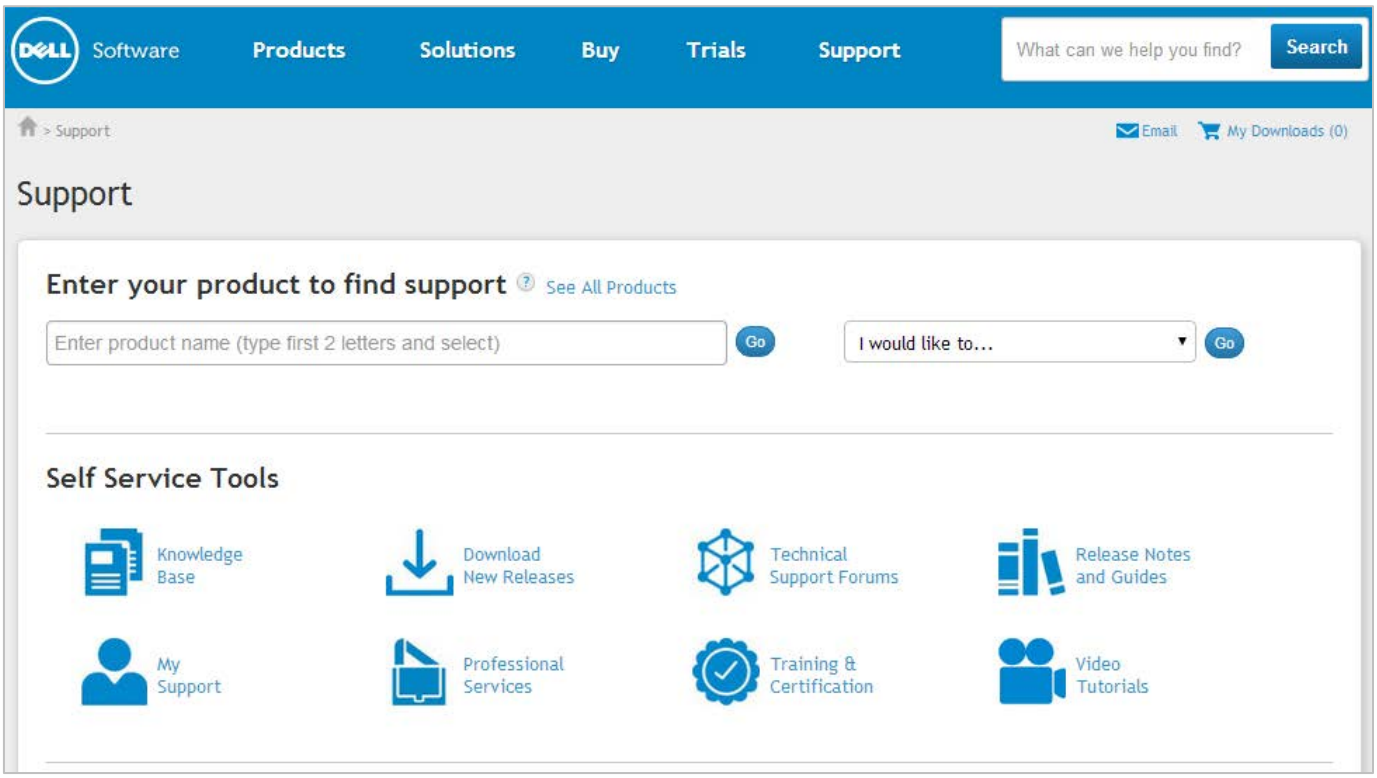
WorkPlace

Symptom	Condition / Workaround	Issue
The user is repeatedly prompted to install Aventail Access Manager.	Occurs after installing the SMA 11.x Secure Endpoint Manager and establishing a successful 11.x WorkPlace session from the client machine, and then disconnecting that WorkPlace session and connecting to a 10.7.1 appliance based WorkPlace session. After logging out and logging in again, the prompt to install AAM is repeated. This issue is observed only when IE11 ActiveX is disabled.	146947

Technical Documentation and the Knowledge Portal

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

Technical documentation, video tutorials, and knowledge base articles are also available on the Dell Software Group Support website: https://support.software.dell.com/.



Last updated: 9/12/2014