Dell Data Protection | Security Tools

Technical Advisories v1.10.1

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

Security Tools Technical Advisories
2016 - 09

Rev. A01

Contents

1

Technical Advisories

Dell Data Protection | Security Tools provides security and identity protection to Dell computer administrators and end users. Security Tools is pre-installed on all Dell Latitude, Optiplex, and Precision computers and on select Dell XPS notebooks. Should you need to reinstall Security Tools, follow the instructions in the *Dell Data Protection | Security Tools Installation Guide*.

This document provides information about Dell Data Protection | Security Tools features and changes in each major release, any issues resolved from a prior release, and any technical advisories in the current release.

Contact Dell ProSupport

Call 877-459-7304, extension 4310039 for 24x7 phone support for your Dell Data Protection product.

Additionally, online support for Dell Data Protection products is available at dell.com/support. Online support includes drivers, manuals, technical advisories, FAQs, and emerging issues.

Be sure to help us quickly connect you to the right technical expert by having your Service Code available when you call.

For phone numbers outside of the United States, check Dell ProSupport International Phone Numbers.

Technical Advisories v1.10.1

Security Tools

- After upgrade to the Windows 10 Anniversary Update, the Challenge/Reponse popup does not display after the user exceeds the maximum allowed attempts to correctly enter the password and answer Recovery Questions on non-UEFI computers with PBA activated. [DDPC-4126]

New Features and Functionality v1.10

- The Windows USB selective suspend feature is now supported.

Resolved Technical Advisories v1.10

Security Tools

- On Dell Latitude 3450 and 3550 computers running Windows 10, fingerprint authentication now proceeds as expected. [DDPC-1598/CSF-772]
- After restoring credentials in Password Manager, a second authentication prompt no longer displays. [DDPC-1617]
- Password Manager logon now functions as expected with Dell Remote Management Console logon. [DDPC-2356]
- Preboot Authentication activation is now prevented on Opal drives with master boot record shadows of less than 128MB. [DDPC-2710]
- Occasionally after the computer hibernates or restarts, enrolled fingerprints must be re-enrolled. [DDPC-2812]

- When the drive letter of a NTFS self-encrypting drive is changed on a computer with Preboot Authentication activated, the computer no longer becomes unresponsive. [DDPC-2973]

Technical Advisories v1.10

Security Tools

- Added 09/2016 - When PBA is activated on a Windows 7 computer without Microsoft Security Advisory 3033929 installed, the computer becomes unstable when resuming from sleep (S3). To work around this issue, install Microsoft Security Advisory 3033929 before installing Security Tools. If Security Tools is already installed, deactivate PBA and uninstall. After installing the Microsoft Security Advisory, reinstall Security Tools. For more information, see https://technet.microsoft.com/en-us/library/security/3033929. [DDPC-4237]

Resolved Technical Advisories v1.9.1

Security Tools

- After upgrade from pre-v1.9 on a computer running Windows 10, fingerprints no longer must be re-enrolled. [CSF-1300, DDPC-1580]
- A non-administrator user can now run an application through User Account Control on a Windows 8, 8.1, or 10 computer with Security Tools installed. [CSF-1313, DDPC-1578]
- Windows password entry now succeeds when entered first in dual-factor authentication on Windows 10, after upgrade to the Windows 10 Fall Update. [DDPC-1675]
- The issue that led to shutdown at PBA login on a computer running ActivClient v7.0.2 is resolved. [DDPC-1898]
- Added 07/2016 - The following Dell computer models are supported with UEFI:

Dell Computer Models - UEFI Support

- Latitude 7370
- Latitude E5270
- Latitude E5470
- Latitude E5570
- Latitude E7240
- Latitude E7250
- Latitude E7260
- Latitude E7265
- Latitude E7350
- Latitude E7440
- Latitude E7450
- Latitude E7460
- Latitude 12 Rugged Extreme
- Latitude 12 Rugged Tablet (Model 7202)
- Latitude 14 Rugged Extreme
- Latitude 14 Rugged
- Precision M3510
- Precision M4800
- Precision M5510
- Precision M6800
- Precision M7510
- Precision M7710
- Precision T3420
- Precision T3620
- Precision T7810
- Optiplex 3040 Micro, Mini Tower, Small Form Factor
- Optiplex 3046
- Optiplex 5040 Mini Tower, Small Form Factor
- OptiPlex 7020
- Optiplex 7040 Micro, Mini Tower, Small Form Factor
- Optiplex 3240 All-In-One
- Optiplex 7440 All-In-One
- OptiPlex 9020 Micro
- Venue Pro 11 (Models 5175/5179)
- Venue Pro 11 (Model 7139)

Resolved Technical Advisories v1.9

Security Tools

- Upgrade from v1.1 and later with PBA activated succeeds. [DDPLP-397]

Technical Advisories v1.9

Security Tools

- To avoid very long installation times due to Windows updates running on Windows 7, ensure that all updates are installed before beginning installation. If Windows KB2913763 is not yet installed, install it then reboot before installing Security Tools. For more information, see https://support.microsoft.com/en-us/kb/2913763. [CSF-847, DDPC-1619]
- In some cases, mapped drives are not available for browsing and selection from the Backup Location page in the Setup Wizard. To work around this issue, enter the fully qualified path into the field in the Backup Location page. [CSF-1057]
- After recovering PBA access through recovery questions, the password change page displays a message that, if no action is taken, the user will be automatically logged in to the Windows session, although no automatic login occurs. [CSF-1083]
- On UEFI computers running the Windows 10 Fall Update and AVG Antivirus, installation is interrupted and never completes. [CSF-1192]
- The fingerprint reader on the Latitude 7510 running Windows 10 loses functionality after upgrade to Windows 10 Fall Update. To work around this issue, perform two restarts and the fingerprint reader will function again. [CSF-1210]
- Occasionally on computers running the Windows 10 Fall Update, fingerprints may need to be re-enrolled. [CSF-1225]
- The Crypto Erase Password policy does not erase the SED but, instead, deletes the authentication tokens for all users and locks the SED. Afterward, only an administrator can forcibly unlock the device. [DDPLP-370, 26862]

Resolved Technical Advisories v1.7.1

Security Tools

- With PBA activated on the Dell Latitude E5250, E5450, and E5550, hibernation now proceeds normally. [CSF-5]
- Single sign-on now succeeds on computers running Windows 7, with installation of the Microsoft KB, https://support.microsoft.com/en-us/kb/2533623. [CSF-788]
- Preboot Authentication now accepts the apostrophe character (') in the username field. [DDPLP-376]

New Features and Functionality v1.7

- The Windows USB selective suspend feature is now supported.

Resolved Technical Advisories v1.7

Security Tools

- Added 11/2015 - The following drives are now supported:

  Drives with "X" are supported but are not qualified for or shipped in Dell systems.

Drive	Availability	Standard
Seagate ST320LT014 (Julius 320GB)	✓	Opal 1
Seagate ST500LM001 (Kahuna 500GB)	✓	Opal 2/eDrive
Seagate ST1000LM015 (Kahuna 1000GB)	✓	Opal 2/eDrive
Seagate ST500LM023 (Yarra X)	✓	Opal 2/eDrive
Seagate ST500LT025 (Yarra R)	✓	Opal 2/eDrive
Seagate ST500LT033 (Asagana)	✓	Opal 2/eDrive
Seagate ST1000DM004 (Desktop 3.5-inch 1000GB)	X	Opal 2/eDrive
Seagate ST1000DM004 (Desktop 3.5-inch 2000GB)	X	Opal 2/eDrive
Seagate ST1000DM004 (Desktop 3.5-inch 3000GB)	X	Opal 2/eDrive
Samsung SM850 PRO 2.5-inch MZ-7KE128 - MZ-7KE2T0 (2.5-inch SED SSD 128GB to 2000GB)	X	Opal 2/eDrive
Samsung SM850 EVO 2.5-inch MZ-75E120-MZ-75E2T0 (2.5-inch SED SSD 120GB to 2000GB)	X	Opal 2/eDrive
Samsung SM850 EVO mSATA MZ-M5E120 - MZ-M5E1T0(mSATA SED SSD 120GB to 1000GB)	X	Opal 2/eDrive
Samsung SM850 EVO M.2. MZ-N5E120- MZ-N5E500(M.2. SED SSD 120GB to 500GB)	X	Opal 2/eDrive
Samsung PM851 OPAL SSD - mSATA (mSATA 128GB - 512GB)	✓	Opal 2/eDrive
Samsung PM851 OPAL SSD - M.2. (M.2. 128GB - 512GB)	✓	Opal 2/eDrive
Micron M500 SSD 2.5-inch (120GB - 960GB)	X	Opal 2/eDrive
Micron M500 SSD mSATA (120GB - 480GB)	X	Opal 2/eDrive

Technical Advisories v1.7

Security Tools

- A warning is truncated on the Encryption screen in the Setup Wizard. The warning advises the user not to unplug or shut down the computer during SED activation. [CSF-579]
- After upgrade from v8.2 or later, authentication with fingerprints fails. To work around this issue, re-enroll fingerprints after upgrade. [CSF-746]
- If activation fails with an error message that the SED must be recovered, perform a recovery using the instructions in the *Recovery Guide*, then reinstall Advanced Authentication and re-activate. [DDPLP-305]
- After uninstallation, the DDP Console icon remains on the desktop. To work around this issue, delete the icon after uninstallation. [DDPMTR-1815]

New Features and Functionality v1.6.1

- Dell Data Protection | Security Tools now supports Windows 10.

Resolved Technical Advisories v1.6.1

Security Tools

- The user can now use the external keyboard, in addition to the virtual keyboard, to submit answers to Recovery Questions. [CSF-332]
- On Windows 10, the issue that occasionally resulted in a blue screen when resuming from sleep on a computer with a SED installed and PBA activated has been resolved. [CSF-363]
- The issue that resulted in unnecessary reboots after the "DellMgmtAgent" service starts is resolved. [CSF-523, CSF-541]

New Features and Functionality v1.6

- Security Tools now provides beta support of Windows 10 Technical Preview.
- The virtual keyboard is now available with Preboot Authentication on the Dell Venue Pro 11 (Model 7139).
- A customer feedback form is now available within the DDP Console. Feedback is delivered to Dell along with the Dell Data Protection product name and version number.

Resolved Technical Advisories v1.6

Security Tools

- In Security Tools - Setup, clicking the **Defaults** button on the Recovery Questions page no longer returns the prompt to confirm deletion of recovery questions but now more accurately prompts the user to confirm a reset of Recovery Questions settings. [CSF-91]
- The System Shutdown Required message that displays before PBA activation begins can now be properly minimized and maximized by clicking the system tray icon. [CSF-195]
- Password Manager now functions properly with Mozilla Firefox v36.0.1 and later. [CSF-199]
- When One-time Password is used to recover access to a computer, if the user enters a blank value for the password, error messages now display "Unknown user name or incorrect password/One or more arguments are not correct." After the user acknowledges the messages, the OTP screen displays. [CSF-233]
- On a German operating system, the PBA logon button text is now sized correctly and fully visible. [DDPLP-276]
- On a UEFI computer with PBA activated and with default Title, Legal Notice, and Support Information for the PBA logon screen, selecting **Options > System Information** no longer returns the message “Support Information is not enabled.” [DDPUP-510]
- On a UEFI computer running a Japanese or Korean operating system with PBA activated, the PBA logon screen now loads and functions as expected. [DDPUP-547]
- On the Dell Precision T1700 and OptiPlex XE2, enabling Secure Boot and activating the PBA no longer results in the error, "No bootable devices found." [DDPUP-614, DDPUP-615]

Technical Advisories v1.6

Security Tools

- When a user begins credential enrollment but quits without saving before enrollment is complete, the credentials are enrolled rather than discarded. To work around this issue, if policy allows the user to modify their own credentials, the user can open the DDP Console, select the **Enrollments** tile, select and delete the credentials. Otherwise, an administrator must remove them. [CSF-146]

- During activation, if the selected backup location is not available, the user cannot set a new backup location in the activation dialog but must instead set the new location through **Administrator Settings > Backup Location** before activation can proceed. [CSF-238]
- Password Manager does not support the Windows 10 web browser, Microsoft Edge. [CSF-281]
- When running on Windows 10, the DDP Console About window displays incorrect BIOS information and an incorrect serial number for the computer's motherboard. [CSF-291, CSF-301]
- When a contactless smart card is moved across the card reader, a popup notification prompts the user to enroll the smart card. If the card is moved multiple times in a short length of time, multiple popup notifications may simultaneously display. [CSF-293]
- On Windows 10, if the Validity Fingerprint Sensor driver is out-of-date, when PBA is activated, the computer experiences a blue screen. To work around this issue, ensure that PBA is not enabled by policy, then follow these steps:

1 Install Dell Data Protection then reboot.
2 In Windows Control Panel, navigate to Device Manager.
3 Under Biometric Devices, disable the Validity Fingerprint Sensor.
4 Activate the PBA.
5 After reboot, the Validity Fingerprint Sensor can be re-enabled, and the fingerprint reader functions as expected.

To download the latest Validity Fingerprint Sensor driver, go to http://www.dell.com/support/home/us/en/19/Products/?app=drivers and select your computer model to check and download the latest driver.

[CSF-349]

- When running Windows 10 on Dell Latitude E7250 or E7450, when the computer resumes from sleep, hibernation, warm boot, or cold boot, the user may be unable to authenticate with an enrolled contactless smart card. To work around this issue, change the policy to require only password authentication. The user should log on and re-enroll the contactless smart card. After re-enrollment, the user will be able to log on with the contactless smart card. [CSF-362]
- Upgrade from v1.1 or v1.2 to v1.6 on a computer with a SED installed and PBA activated fails. To work around this issue, first upgrade to v1.5 then upgrade to v1.6. [CSF-449, CSF-461]
- Added 08/2015 - If Microsoft TPM Base Services is improperly installed, the following functionality is affected: HCA provisioning, fingerprint enrollment in the DDP Console/Security Console, and BitLocker Manager operation. For more information and to work around this issue, refer to this KB article: http://www.dell.com/support/article/us/en/19/SLN296706. [CSF-454]
- Upgrade on a computer with a LiteOn M3 series SSD installed and PBA activated fails due to the small disk size. To work around this issue, before upgrading, deprovision the PBA. After upgrade, the PBA can be reactivated. [CSF-528]
- With PBA activated on Dell Latitude E7450, navigation of the Advanced Boot Options menu is not possible because the native keyboard is not available. To work around this issue, deactivate the PBA, access the Advanced Boot Options menu, and keyboard navigation is available. [DDPLP-286]
- On Dell Latitude E7250, E7350, E7450, and Venue Pro 11 (Model 7139), recovery fails with Dell Opal SED Recovery Utility one-time unlock of the drive. To work around this issue, use the recovery key to unlock a drive on one of these models. [DDPUP-763]

Resolved Technical Advisories v1.5.1

Security Tools

- Occasional upgrade failures from Security Tools to Enterprise Edition have been resolved. If the initial upgrade fails due to the Server being unavailable, the client will continue to be locally managed until the Server can be contacted and a new policy set is received at the client. [CSF-1]
- When using Security Tools, the enrollment credentials wizard summary page now shows the chosen login option in the summary. [CSF-93]
- When using Security Tools' One-time Password feature, for devices that are already enrolled, enrollments are now properly deleted when the policy "Mobile Device Require Password" is changed from Off to On. [CSF-94]
- When using Security Tools' One-time Password feature, null reference pointers have been resolved. [CSF-98]
- The issue of using Security Tools, Windows 8.1, and the GPO "Do Not Display Last Username", causing single sign-on to fail has been resolved. [CSF-100]

- Improvements have been made to make user login and start-up more reliable. [CSF-114, CSF-116]
- Issues related to the "DellMgmtAgent" service failing to start or starting slowly have been resolved. These issues presented in the Windows System Event Viewer under the Service Control Manager with a message similar to the following: "The DellMgmtAgent service failed to start due to the following error: The service did not respond to the start or control request in a timely fashion." [CSF-116]
- Encryption statistics now properly display in the Security Tools Console. [CSF-121]
- Enhancements have been made to the installer to ensure that the correct PBAAuthURI is maintained, even if the installation reboot occurs before the authentication agent is upgraded. [CSF-123, CSF-125]
- The issue of “Security Tools - Setup” being incorrectly translated in Chinese to “Security Tools - Installation” has been resolved. [CSF-128]
- When running Security Tools, “DDP Console – Admin Settings” is now properly displayed in the All Programs menu instead of NewShortCut3. [CSF-129]
- The issue of failing attempts to open a Microsoft Excel workbook, with either a message that a problem occurred sending the command to the program or a message that the file path or file name could not be found, is now resolved. [CSF-157]
- The size of the Security Tools Console now stays constant, unless it is manually enlarged or reduced. [DCF-2]
- The issue of some special unicode characters, particularly German language umlaut characters, failing to be recognized during entry of password recovery questions, is resolved. [DDPLP-202]

New Features and Functionality v1.5

- Preboot Authentication (PBA) with password is now supported on Windows 8 and Windows 8.1 on select Dell UEFI computers with qualified Opal Compliant SEDs.
- Secure Boot is now supported with the Encryption client and Security Tools on select Dell UEFI computers running Windows 8 and Windows 8.1 with qualified Opal Compliant SEDs.
- Manual entry One-time Password (OTP) is now supported for Windows logon and recovery of access to computers running Security Tools.

Resolved Technical Advisories v1.5

Security Tools

- On Dell Venue tablets, after the Enrollment Wizard is launched, the on-screen keyboard can now be opened by tapping the keyboard icon in the Wizard or the keyboard system tray icon. [MMW-524]
- On computers with Intel Rapid Start, the hibernation partition no longer has to be removed in order for the SED management client/Security Tools to function properly. [28562/MMW-701]

Technical Advisories v1.5

Security Tools

- On a UEFI laptop computer with the PBA activated, when the computer is docked or attached to an external monitor, the laptop lid must remain open in order for the PBA to function properly. [DDPUP-507]
- Password Manager does not support Google Chrome v35 and later, due to a change in the way Chrome handles extensions. [MMW-619, MMW-754]
- During an update to Intel Rapid Storage Technology Drivers, the self-encrypting drive may become undetectable. To resolve this issue, reboot the computer a second time after the update has been applied. [MMW-633]
- During installation and the post-installation restart, if an external drive is removed from the computer, the computer will not reboot. To work around this issue, shut down the computer and reconnect the external drive. Power on the computer. The computer will boot normally. [MMW-693]
- On a computer with multiple users the Windows Power Option, Require a password on wakeup, must be enabled. If this option is not enabled, when the computer resumes from hibernation, it resumes in the user account in which hibernation occurred. This behavior is typical of Windows hibernation. [MMW-761]
- Password Manager does not support importing credentials from Internet Explorer 10 and 11 (because the interface is not published by Microsoft). [MMW-770]

- On computers running ActivClient 7, single sign-on may not function properly. Also, multiple smart card icons may display in the Windows credential provider screen. [MMW-837]
- After activating Preboot Authentication on a UEFI computer, when the computer resumes from hibernation for the first time following PBA activation, the process becomes a cold boot. After the first hibernation, the computer resumes from hibernation normally. To work around this issue, restart the computer a second time after PBA activation. [MMW-844]
- When Preboot Authentication is activated on a computer with more than one user and with only fingerprint authentication enabled, if two or more users enroll with the same fingerprint, at authentication for second and subsequent users an error message may display, "The fingerprint is not verified." However, the first user is able to authenticate successfully. [MMW-848]
- Eikon external fingerprint readers do not function properly on Windows 8.1 without the latest drivers. To work around this issue, when using an external fingerprint reader, download and install the latest drivers required for your specific reader. [MMW-880]

New Features and Functionality v1.4.1

- Multi-certificate Common Access Cards are now supported.

Resolved Technical Advisories v1.4.1

Security Tools

- Previously, when using a non-USH external fingerprint reader, after the computer went to sleep or was rebooted, logon using fingerprint failed. The issue with the credential provider timing out when attempting to confirm the fingerprint reader is connected to the computer is resolved. [28605, MMW-360]
- Previously, when upgrading, an error message displayed indicating that ushradiomode64.exe was not able to start correctly. The issue of a third-party installer incorrectly attempting to install Microsoft .Net Framework 3.5 on the computer is resolved. [29049, DDPC-182, MMW-357]
- Previously, on some computers with Security Tools and Preboot Authentication enabled, the computer would not boot after entering credentials into the PBA logon screen, and the computer would halt at a black screen with the words "Parity Error". [DDPLP-137]

Technical Advisories v1.4.1

Security Tools

- Single Sign-on intermittently fails on computers with self-encrypting drives on which Preboot Authentication is activated. [DDPLP-144]
- When replacing a provisioned self-encrypting drive (with the Preboot Authentication environment active) with a *new* self-encrypting drive and provisioning the Preboot Authentication environment, after the new SED is provisioned, the old SED can no longer be recovered. [DDPLP-150, MMW-581]
- On the Dell Latitude Rugged Extreme, the user is able to detach the tablet from the dock. However, the dock is needed to log in through the PBA. Detach the tablet only after the PBA authentication step is complete. [DDPLP-162, DDPLP-163]
- Fingerprint enrollment does not prevent the user from using fingerprints from different fingers when enrolling a single finger. [MMW-212]
- Single Sign-on is not available when using multi-certificate CACs. [MMW-559]
- After successfully authenticating to the Preboot Authentication environment, the computer will not complete Single Sign-on. Instead, the computer halts at the Windows Logon screen for another user. Microsoft Windows 8.1 defaults to the Logon screen for the previously authenticated user. To complete logon, return to the User Tiles screen by selecting the back arrow in the top right of the screen and then selecting the correct user tile for the user authenticated in the PBA. SSO data captured by the PBA may still be present and once the user tile is selected, Windows authentication may be completed automatically. [MMW-564]

Resolved Technical Advisories v1.4

Security Tools

- Pre-enrolled Contactless Smart Card users are no longer lost after joining the computer to the domain. [28386/DDPC-61, MMW-347]

Resolved Technical Advisories v1.3.2

Security Tools

- A new user is no longer presented a logon screen for a different user when logging on to the PBA for the first time with dual-factor authentication configured for Password + Fingerprints. [28886]
- Fingerprint credentials are now retained when upgrading from v1.2.1 or earlier. [28457, 28766]
- Upgrade failures related to a USH fingerprint sensor configuration file error have been resolved. [28845]
- Attended enrollment is no longer needed when the Authentication Policy is set to Fingerprints + Contactless Smart Cards. [28873]

Technical Advisories v1.3.2

Security Tools

- There are no new technical advisories in ST 1.3.2.

Resolved Technical Advisories v1.3.1

Security Tools

- There are no resolved technical advisories in ST 1.3.1.

Technical Advisories v1.3.1

Security Tools

- There are no new technical advisories in ST 1.3.1.

New Features and Functionality v1.3

- Dell Data Protection | Security Tools now supports Windows 8 and Windows 8.1 using legacy boot mode for all computers configured with an SED.

Resolved Technical Advisories v1.3

Security Tools

- After uninstallation, all folders are now properly removed. [26037]
- During password recovery, when answers to Recovery Questions are entered, the answers now display as obfuscated characters rather than in clear text. [27977]
- Computers on which Preboot Authentication is activated now display the PBA screen as expected after resuming from Fast Boot, Shutdown, Hibernate, and Hybrid Sleep. [28082, 28090]
- The fingerprint reader no longer fails at sign on due to Microsoft Windows fingerprint reader private sensor pool issues. [28085]
- In the Administrator Console, the scroll bar now functions properly on the Dell Latitude E6440 running Microsoft Windows 8.1. [28298]
- In landscape view on Dell Venue tablets, buttons and the side scroll bar now display correctly on all screens. [28346, 28347]
- On French operating systems, version information that is displayed in the Security Console > Settings > About page is now correct. [28385]
- The first time after activation of Preboot Authentication, if the computer is locked (CTRL+ALT+DEL) after the "System Shutdown Required" message displays and then the user unlocks the computer, the "System Shutdown Required" message now correctly displays again. A restart is no longer required. [28391]

Technical Advisories v1.3

Security Tools

- Preboot Authentication format must be domain\user for domain credentials.
- The computer does not Single Sign-on (SSO) after waking up from Hybrid Sleep. After the user enters their credentials at the Preboot Authentication (PBA) screen, the computer stops at the Windows logon screen and the user must manually log on to the computer.

  Dell Data Protection | Security Tools and Dell Data Protection | Encryption do not support Hybrid Sleep states and SSO when Preboot Authentication (PBA) is Active. Disable Hybrid Sleep when using Preboot Authentication if your organization intends to use SSO. [25785]
- Removing the USB Fingerprint reader without ejecting the device causes Dell ControlVault to fail. The issue occurs because Windows handles the removal action of biometric devices incorrectly. To correct this issue, download and install the Hotfix available at http://support.microsoft.com/kb/2913763. [27696]
- Windows logon fails with some new CAC smart cards, which use multiple certificates with the same name. One certificate is the authentication certificate and the other is a signing certificate. The algorithm used to select the certificate uses the newest certificate. If the newest certificate is the signing certificate, Windows logon will fail. To work around this issue, create an Active Directory entry for the principle name for the signing certificate. [27857]
- The "Delete User" functionality does not work after PBA recovery. During PBA recovery, the PBA is removed. Attempting to delete users using the Administrator Console fails because the PBA has already been removed. To work around the issue, do not remove users from the Administrator Console after the PBA is recovered. Instead, remove users from a recovered PBA by uninstalling and re-installing Security Tools. [27973]
- On laptops with battery charges of 10 percent or less, the Dell Data Protection installation process will stop even when the computer is connected to a power source. To work around this issue, ensure that the battery charge is at least 50 percent before beginning installation. [27974]
- A contactless card may not be immediately recognized, because Windows does not load its driver. To work around this issue, in Windows Device Manager, disable the smart card device. For more information, see http://support.microsoft.com/kb/976832. [27981]
- All registry keys and installation files are not removed after uninstallation. [28219]
- On Dell Venue tablets, the touch keyboard is not automatically available at the Windows logon screen. To work around this issue, touch the keyboard icon to display the touch keyboard. [28257]

- Preboot Authentication fails if a self-encrypting drive is configured as drive 1. To work around this issue, configure a self-encrypting drive as the boot drive (drive 0) for Preboot Authentication to function properly. [28266]
- The shortcut to the Administrator Console disappears after initial settings are configured. [28396]
- Due to a Microsoft issue with Windows 2000 or 2003 Domain Controllers or 2008 Mixed Mode Domain Controllers, users cannot change an expired password or reset a password to be changed at next logon. To work around the issue, an Administrator can reset the user's password and deselect "Change Password at Next Logon" in Active Directory. When users log on, they can change their passwords using CTRL-ALT-DEL and selecting "Change password...". The following operating systems are affected:

  Windows 8 (with KB2883201 installed)

  Windows 8.1

  [28501]
- When the Password Manager option, Fill in logon data, is selected and credentials are enrolled with Password Manager, data is populated into a logon screen but log on does not occur. [28502]
- With Windows 8.1, after a Password Manager logon is deleted in the Security Console, the link to the logon page remains in the list of Password Manager logons. [28515]
- Password Manager is not available in Google Chrome until it is activated. To activate Password Manager in Google Chrome, follow these steps:

1 In the Google Chrome Settings page, select **Make Google Chrome my default browser**.

2 Select **Show advanced settings** > **Content settings** > **Disable individual plug-ins** and then select **Always allowed** for the Dell Data Protection | Security Tools Plug-in. Close the Plug-ins page.

3 In the Google Chrome Settings page, select **Extensions** and check the Enable box next to the Dell Data Protection | Security Tools Extension.

4 Exit Google Chrome and re-launch.

When you access a site that contains a logon form you will be prompted with the pre-train icon to capture the logon credentials for the site.

[28528, 28678, 28719]

- In Password Manager, the Select Logon Data window does not show the user name of the first enrolled user. [28531]
- Preboot Authentication uses a "Basic" disk partition and cannot be converted to "Dynamic" partition (for RAID arrays). Attempts to convert the partition will result in the PBA not being created or the PBA not starting. [28587]
- After Preboot Authentication is deactivated, the Administrator and Security Consoles do not immediately reflect the deactivation. To work around this issue, restart the computer. After the restart, the Administrator and Security Consoles correctly indicate that Preboot Authentication is deactivated. [28604]
- When removable media is used for backup, recovery keys are not generated when the root directory is selected as a backup location. To work around this issue, select a folder, rather than the root directory, as backup location. [28650]
- When using Password Manager with Firefox, double-clicking the pre-train icon does not open the Add Logon dialog. [28693]
- After installation of Security Tools, the Microsoft Usbccid Smartcard Reader is intermittently reported as being in a problem state in Device Manager. However, smart cards and fingerprints seem to function normally. Dell ControlVault relies on the Microsoft Usbccid drivers. A premier case has been opened with Microsoft regarding this issue. [28697]
- The Password Manager shortcut (CTRL+WIN+H) cannot be used on tablets, because the WIN button is not present. [28706]
- Some USB 3.0 drives cannot be used for backup, because they appear to the operating system to be internal drives. Internal drives cannot be used as backup locations. If you use a USB 3.0 drive and Windows registers it as an internal drive, use a network location or USB 2.0 drive for backup rather than the USB 3.0 drive. [28707]
- Password Manager prompts for credentials only when accessed for the first time after the user logs on and not again until the next log on or computer restart. This is working as designed. [28714]
- Infrequently, the Security Tools installer returns an error "The operation was canceled by the user." To work around this issue, retry the installation. [28729]
- With Windows 8.1, the dialog windows of the Security Tools installer flicker. [28730]
- Moving a self-encrypting drive with Preboot Authentication activated to a different computer may result in loss of data on the drive. To avoid such data loss, immediately perform a Recovery to deactivate PBA. Recovery must be performed and PBA must be deactivated before any settings are changed in the Administrator Console. [28735]

- After user enrollments are removed in the Administrator Console, the logon screen still reflects Security Tools as managing authentication credentials. [28740]
- If more than 36 characters are entered as a title In the Administrator Console Preboot Authentication Custom Logon policy, the Log In button on the Preboot Authentication screen is hidden. When this issue is present, a user can still enter credentials and log in using the Enter key in place of the Log In button. To work around this issue, ensure that Custom Logon title text is no longer than 36 characters. [28782]
- Secure Boot is a Unified Extensible Firmware Interface (UEFI) protocol that Windows 8 and 8.1 users can enable in the computer's BIOS to ensure that the computer boots using trusted firmware signed by the computer manufacturer. The feature is not supported when the following conditions are met:

  - SED with Dell Data Protection | Security Tools installed
  - SED with Dell Data Protection | Encryption installed
  - SED with Dell Data Protection | Security Tools and Dell Data Protection | Encryption installed
  - HCA with Dell Data Protection | Security Tools installed
  - HCA with Dell Data Protection | Encryption installed
  - HCA with Dell Data Protection | Security Tools and Dell Data Protection | Encryption installed

  To upgrade to Windows 8 or 8.1 on a Dell computer with SED or HCA, Secure Boot cannot be enabled in BIOS. The Secure Boot setting is disabled by default for computers shipping with Windows 7 or Windows 8/8.1 Downgrade Rights. This setting should not be changed.

  Instructions:

  a Turn on the power to your Dell computer. If the computer is already powered on, reboot it.
  b Press **F2** or **F12** continuously during boot until a message displays at the upper right of the screen that is similar to "preparing to enter setup" (F2) or "preparing one-time boot menu" (F12). This launches the system BIOS.
  c In Setting > General > Boot Sequence, ensure that the Legacy Boot List Option is selected.
  d In Settings > General > Advanced Boot Options, ensure that the Enable Legacy Options ROMs check box is selected.
  e In Settings > Secure Boot > Secure Boot Enable, ensure that the Secure Boot Enable selection is Disabled.
  f Apply the changes.
  g Now that the computer BIOS has been changed to legacy boot mode, the computer must be re-imaged.

  [28790]
- When Security Tools Authentication components are uninstalled, the user is not warned that Preboot Authentication is provisioned. Uninstalling Security Tools Authentication will impact only the user's ability to update credentials in the PBA but will not prevent the user from authenticating with existing user accounts. The proper uninstallation sequence is as follows:

  Deactivate the PBA

  Uninstall Security Framework

  Uninstall Security Tools Authentication

  [28791]
- The Password Manager version number may differ across web browsers. [28808]
- Amended 05/2014 - Attempting to upgrade from Dell Data Protection | Security Tools 1.0.0 or 1.0.1 to the latest release fails and an error message is displayed saying that the computer has not been modified. This issue occurs because the installer cannot deactivate the PBA and, therefore, uninstallation of the earlier version is blocked. To work around this issue, deactivate the PBA and reboot the computer before attempting to upgrade to the new version. [28817]
- The user is not prompted to enroll authentication credentials although the Logon Policy is set to prompt after the configured length of time. [28841]
- In the Security Console, the Backup and Restore feature is described as providing data backup and restore functions but is specifically related to backup and restore of Password Manager data. [28856]
- The Dell Optiplex XE2 computer intermittently does not display the Windows logon or credential provider screen after waking from sleep. To work around this issue, upgrade to the latest applicable BIOS version, which is A05 as of 03/2014. In the BIOS screen, locate the option for Deep Sleep and disable it. [28862]

- After locking the computer with CTRL-ALT-DELETE, when the computer is unlocked with a password or fingerprint, a message that reads "Locking" displays before the computer is unlocked. [28896]
- Hybrid Sleep is not supported on Windows 8.1 with SED drives on the Precision M6800/M4800 platform. [28897]
- When dual-factor authentication is enabled and the computer resumes from sleep, the computer intermittently stops responding and the screen is black. To recover from this situation press and hold the power button until the computer shuts down, then reboot the computer. [28900]

Resolved Technical Advisories v1.2.1

Security Tools

- Dell Data Protection | Security Tools provides improved support for the touch keyboard on the Microsoft Windows 8.1 Sign On Screen.
- When using Microsoft Windows 8.1, the Security Console screen will no longer be blank after minimizing and re-opening the window. [28044]
- Amended 03/2014 - Password Manager pre-train icons are now supported with Google Chrome and Mozilla Firefox as well as Internet Explorer when using Microsoft Windows 8.1. However, Password Manager is not available in Google Chrome until it is activated. To activate Password Manager in Google Chrome, follow these steps:

1 In the Google Chrome Settings page, select **Make Google Chrome my default browser**.

2 Select **Show advanced settings** > **Content settings** > **Disable individual plug-ins** and then select **Always allowed** for the Dell Data Protection | Security Tools Plug-in. Close the Plug-ins page.

3 In the Google Chrome Settings page, select **Extensions** and check the Enable box next to the Dell Data Protection | Security Tools Extension.

[28329]

Technical Advisories v1.2.1

Security Tools

- Amended 03/2014 - When using Microsoft Windows 7 on the All-in-One computer without an external keyboard, the On-Screen Keyboard does not automatically display after the computer resumes from the sleep or hibernate state. To display the On-Screen Keyboard, select the On-Screen Keyboard button at the lower left of the Windows Login Screen. [28606]
- Amended 04/2014 - Integrated fingerprint readers on Latitude E6430u and Latitude E5430 do not work after installing Dell Data Protection | Security Tools 1.2.1 or later on Windows 7 (64-bit). To use the integrated fingerprint reader on these computer models, use Dell Data Protection | Security Tools 1.2 (or Dell Data Protection | Encryption 8.2). [28979/DDPC-157, MMW-393]

New Features and Functionality v1.2

- Microsoft Windows 8.1 is now supported on X5 platforms.

Resolved Technical Advisories v1.2

Security Tools

- The Crypto Erase Password policy now erases the SED instead of locking it. [26862]
- When using the Administrator Console, intermittent refresh issues no longer occur when setting the recovery questions. [27036]
- The PBA authentication process times on Samsung drives have been improved. [27318]

- Upon opening the Administrator Console the first time after installation, blank DPTrace.dll files no longer display on the desktop. [27539]

Technical Advisories v1.2

Security Tools

- Some keys in the registry and some installation files are not removed at uninstallation. [28219, 27475]
- A message that reads “Please do not turn off or unplug your computer” persists on the Dell Latitude E6440 running Microsoft Windows 7 (32-bit). [28245]
- Amended 01/2014 - When using Microsoft Windows 8.1, Single Sign-On with Password Manager does not work with some email providers. [28259]
- Amended 01/2014 - The Password Manager prompt to add a login screen displays after de-selecting "Prompt to add logons for logon screens" in the Security Console Settings or when selecting "Exclude this screen" in Internet Explorer Icon Settings. To correct the issue, download and install Microsoft KB2888505 https://support.microsoft.com/kb/2888505. [28334, 28445, 28536]
- Touch capability is not available for Password Manager icons on Dell Venue Pro 11 and Dell Venue Pro 8 tablets.
- Updated drivers for the Eikon to Go external fingerprint reader for Windows 8.1 can be found on support.dell.com.

Resolved Technical Advisories v1.1

Security Tools

- The Tab key can now be used to navigate through the recovery questions in the Security Console. [26974]
- When using Password Manager, the default values in the Live.com/Hotmail.com credential fields are now correct. [27033]
- The Authentication tab in the Security Console no longer displays a blank page after switching tabs. [27112]

Technical Advisories v1.1

Security Tools

- Amended 03/2014 - The computer does not Single Sign-on (SSO) after waking up from Hybrid Sleep. After the user enters their credentials at the Preboot Authentication (PBA) screen, the computer stops at the Windows logon screen and the user must manually log on to the computer.

  Dell Data Protection | Security Tools and Dell Data Protection | Encryption do not support Hybrid Sleep states and SSO when Preboot Authentication (PBA) is Active. Disable Hybrid Sleep when using Preboot Authentication if your organization intends to use SSO. [27496, 25785]
- When using a Precision M6800, Single Sign-On will fail if a USB device is currently plugged into the computer. [27595]
- Added 03/2014 - Single Sign-On does not work on computers with self-encrypting drives. To work around this issue, upgrade to Dell Data Protection | Security Tools v1.3. [28586]

Resolved Technical Advisories v1.0

Security Tools

- There are no resolved technical advisories in ST v1.0.

Technical Advisories v1.0

Security Tools

- When uninstalling Dell Data Protection | Security Tools, an error may display stating, "An error occurred while trying to uninstall DDP|CSF." You may safely dismiss this error. The application will refresh, and Client Security Framework (CSF) will be properly uninstalled. [26866]
- When using the Administrator Console, intermittent refresh issues have been observed when setting the recovery questions. Resize the window to correct the issue. [27036]
- Dell Data Protection | Security Tools cannot be installed when Dell Data Protection | Access is present on the computer. Follow the steps in the Dell Data Protection | Security Tools Installation Guide to uninstall DDP|A. [27073]

Software and Hardware Compatibility

Dell Data Protection | Security Tools is tested with third-party software and hardware as needed. Dell reports problems found during testing to other vendors, where appropriate.

AVG Antivirus Protection

- On UEFI computers running the Windows 10 Fall Update and AVG Antivirus, Advanced Authentication installation is interrupted and never completes. [CSF-1192]

Hacks and Utilities

- Hacks or utilities that alter device manufacturer performance specifications are not supported. For example, the AfterBurner hack adjusts the clock speed of a device processor, affecting the results of certain math operations. Because some of these math operations are required for encryption and decryption, using this hack could lead to data corruption.