# Installation of Dell Data Protection | Security Tools after point of sale on Dell Latitude™, Optiplex™ and Precision Systems

Installation Guide

August 2013

# Introduction

Dell Data Protection | Security Tools (DDP | ST) enables local management and provisioning of Dell's advanced authentication hardware and self-encrypting drives and provides new policy options to better secure your Dell endpoints.

# Dell Data Protection | Security Tools Compatibility

## Dell Data Protection | Access

Dell Data Protection | Access (DDP | A) is not compatible with DDP | ST. As both products manage your advanced authentication hardware and self-encrypting drives (SEDs), you cannot run both simultaneously. If you would like to install DDP | ST, you will need to uninstall DDP | A. For a numbered list use the "Numbered(1)" style.

## Dell Data Protection | Encryption 7.2.x

Dell Data Protection | Encryption (DDP | E) version 7.2.x is compatible with DDP | ST, but you will not realize the full potential of DDP | ST with DDP | E 7.2.x. Dell recommends that you upgrade to DDP | E 8.x to enable full, integrated remote management of your authentication policy within the DDP | E remote console.

## Dell Data Protection | Encryption 8.x

Dell Data Protection | Encryption 8.x was designed to work with and augment the features of DDP | ST. The DDP | E remote management console provides the ability to remotely manage all of the authentication policies which can be locally managed within the DDP | ST local console.

# Installation of DDP | ST on a Platform with DDP | A

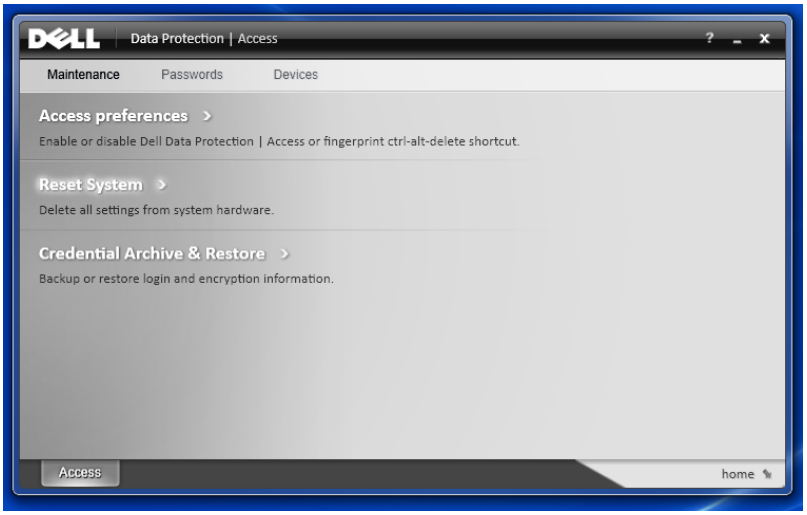
If you attempt to install DDP | ST on a system that has DDP | A installed, you will receive an error message advising you of the incompatibility with DDP | A. This error message provides basic guidance for uninstalling DDP | A. Following acknowledgement of this error message, the installation will abort. More detailed instructions are provided here.

Prior to uninstalling DDP | A, you must deprovision any hardware managed by DDP | A. Note: If using some encryption products, such as DDP | E 7.2.x or Microsoft Bitlocker™, you will also need to stop or pause your encryption policy.

Deprovisioning DDP|A managed hardware includes the fingerprint reader, smart card reader, bios passwords, TPM and the self-encrypting drive. If you have not used DDP | A, you may uninstall DDP | A and restart the DDP | ST installation process.

## Deprovision DDP | A Managed Hardware

Launch DDP | A and click on the Advanced Tab.




Select Reset System. This will require that you enter any provisioned credentials to verify your identity. After DDP | A verifies the credentials, DDP | A will perform the following actions:

1. Remove all provisioned credentials from Dell ControlVault ™ if present
2. Remove Dell ControlVault ™ owner password, if present
3. Remove all provisioned fingerprints from integrated fingerprint reader, if present
4. Remove all BIOS passwords (BIOS System, BIOS Admin, and HDD passwords), and
5. Clear the Trusted Platform Module
6. Remove the DDP | A Credential Provider

Once these devices are deprovisioned, DDP | A will reboot the system to restore the Windows default Credential Provider.

## Uninstall DDP | A

Once your authentication hardware is deprovisioned, you can uninstall DDP|A. Navigate to Control Panel > Programs and Features and select Dell Data Protection | Access. Click "Uninstall" to launch the installer. When the installer finishes removing the files, click "Yes" to reboot.

If using a self-encrypting drive, removing DDP | A will also unlock the SED and remove the pre-boot authentication.