Dell Data Protection

控制台用户指南

加密状态
身份验证注册
Password Manager
版本 1.10

© 2016 Dell Inc.

Dell Data Protection | Encryption、 Dell Data Protection | Endpoint Security Suite、 Dell Data Protection | Endpoint Security Suite Enterprise、Dell Data Protection | Security Tools 和 Dell Data Protection | Cloud Edition 整套文件中使用的注册商标和商标：Dell™ 和 Dell 徽标、Dell Precision™、OptiPlex™、ControlVault™、Latitude™、XPS® 和 KACE™ 是 Dell Inc. 的商标。Cylance® 和 Cylance 徽标是 Cylance, Inc. 在美国和其他国家 / 地区的注册商标。 McAfee® 和 McAfee 徽标是 McAfee, Inc. 在美国和其他国家 / 地区的商标或注册商标。Intel®、Pentium®、Intel Core Inside Duo®、Itanium® 和 Xeon® 是 Intel Corporation 在美国和其他国家 / 地区的注册商标。Adobe®、Acrobat® 和 Flash® 是 Adobe Systems Incorporated 的注册商标。Authen Tec® 和 Eikon® 是 Authen Tec 的注册商标。 AMD® 是 Advanced Micro Devices, Inc. 的注册商标。 Microsoft®、 Windows® 和 Windows Server®、 Internet Explorer®、 MS-DOS®、 Windows Vista®、 MSN®、 ActiveX®、 Active Directory®、 Access®、 ActiveSync®、 BitLocker®、 BitLocker To Go®、 Excel®、Hyper-V®、Silverlight®、Outlook®、PowerPoint®、OneDrive®、SQL Server® 和 Visual C++® 是 Microsoft Corporation 在美国和 / 或其他国家 / 地区的商标或注册商标。VMware® 是 VMware, Inc. 在美国和其他国家 / 地区的注册商标或商标。Box® 是 Box 的注册商标。 Dropbox℠ 是 Dropbox, Inc. 的服务标记。 Google™、 Android™、 Google™ Chrome™、 Gmail™、 YouTube® 和 Google™ Play 是 Google Inc. 在美国和其他国家 / 地区的商标或注册商标。 Apple®、 Aperture®、 App Store℠、 Apple Remote Desktop™、Apple TV®、Boot Camp™、FileVault™、iCloud®℠、iPad®、iPhone®、iPhoto®、iTunes Music Store®、Macintosh®、Safari® 和 Siri® 是 Apple, Inc. 在美国和 / 或其他国家 / 地区的服务标记、商标或注册商标。 GO ID®、 RSA® 和 SecurID® 是 EMC Corporation 的注册商标。EnCase™ 和 Guidance Software® 是 Guidance Software 的商标或注册商标。Entrust® 是 Entrust®, Inc. 在美国和其他国家 / 地区的注册商标。 InstallShield® 是 Flexera Software 在美国、中国、欧盟、中国香港、日本、中国台湾和英国的注册商标。 Micron® 和 RealSSD® 是 Micron Technology, Inc. 在美国和其他国家 / 地区的注册商标。 Mozilla® Firefox® 是 Mozilla Foundation 在美国和 / 或其他国家 / 地区的注册商标。iOS® 是 Cisco Systems, Inc. 在美国和某些其他国家 / 地区的商标或注册商标，并在授权下使用。Oracle® 和 Java® 是 Oracle 和 / 或其附属公司的注册商标。其他名称可能为其各自所有者的商标。 SAMSUNG™ 是 SAMSUNG 在美国或其他国家 / 地区的商标。 Seagate® 是 Seagate Technology LLC 在美国和 / 或其他国家 / 地区的注册商标。 Travelstar® 是 HGST, Inc. 在美国和其他国家 / 地区的注册商标。 UNIX® 是 The Open Group 的注册商标。 VALIDITY™ 是 Validity Sensors, Inc. 在美国和其他国家 / 地区的商标。 VeriSign® 和其他相关标志是 VeriSign, Inc. 或其附属公司或子公司在美国和其他国家 / 地区的商标或注册商标，并授权给 Symantec Corporation。 KVM on IP® 是 Video Products 的注册商标。 Yahoo!® 是 Yahoo!Inc. 的注册商标。

此产品使用部分 7-Zip 程序。在 www.7-zip.org 中可以找到源代码。许可基于 GNU LGPL 许可证 + unRAR 限制 (www.7-zip.org/license.txt)。

2016-07

受一项或多项美国专利保护，包括：No. 7665125 ； No. 7437752 ；以及 No. 7665118。

本文档中的信息如有变更，恕不另行通知。

目录

1 简介 5

2 DDP 控制台 7

3 加密状态 9

4 注册 11

首次注册凭据 **11**

添加、修改或查看注册 **11**

密码 **11**

恢复问题 **12**

指纹 **12**

移动设备 **13**

设置 Security Tools Mobile 13

配对移动设备和计算机 13

注册另一台移动设备 14

取消计算机与移动设备配对 14

使用一次性密码登录 **15**

Security Tools Mobile 管理任务 **15**

重设 Security Tools Mobile 应用的 PIN 15

卸载 Security Tools Mobile 应用 15

智能卡 **16**

5 Password Manager 17

Password Manager 入门 **17**

管理登录 **17**

添加类别 18

添加登录 18

导入凭据 **18**

图标上下文菜单 **19**

登录到已设定的登录页面 **19**

Web 域支持 **20**

填充 Windows 凭据 **20**

排除网站 **20**

禁用设定登录表单提示 **21**

备份和还原 Password Manager 凭据 **21**

备份凭据 21

还原凭据 21

词汇表 23

1

简介

Dell Data Protection | Security Tools 提供了直观易用的工具，用于增强计算机的安全性。

以下是可通过 DDP 控制台使用的功能：

- 注册用于 Security Tools 的凭据。
- 充分利用多重凭据，包括密码、指纹和智能卡
- 在忘记密码时，可以恢复对计算机的访问，而无需呼叫服务台或管理员协助
- 备份和还原程序数据
- 轻松更改 Windows 密码
- 设置个人首选项
- 查看加密状态 （适用于配备自加密驱动器的计算机）

DDP 控制台

DDP 控制台 界面可用于注册和管理凭据，以及配置自恢复问题。

您可以访问以下应用程序：

- “ 加密状态 ” 工具可用于查看计算机驱动器的加密状态。
- “ 注册 ” 工具可用于设置和管理凭据，配置自恢复问题，以及查看凭据注册的状态。由管理员设置您可以注册的各类凭据。
- Password Manager 可用于自动填写和提交登录网站、 Windows 应用程序和网络资源所需的各种数据。 Password Manager 还允许通过应用程序更改登录密码，确保 Password Manager 所维护的密码与目标资源的密码保持同步。

本指南介绍如何使用这些应用程序。

请确保定期检查 dell.com/support 以获取最新说明文件。

联系 ProSupport

在联系 Dell ProSupport 以获取帮助前，请确保在致电时提供服务标签来帮助我们使您与正确的技术专家取得快速联系。

要联系 ProSupport，请致电 877-459-7304 （分机号 4310039）以获取针对 Dell Data Protection 产品的全天候电话支持。

另外， Dell D.ata Protection 产品的联机支持位于 dell.com/support。联机支持包括驱动器、手册、技术咨询、常见问题以及出现的问题。

2

DDP 控制台

DDP 控制台 为计算机的所有用户提供对确保安全性的应用程序的访问，以查看和管理计算机的驱动器和分区的加密状态，根据管理员设置的策略管理对网站、程序和网络资源的登录信息；以及轻松注册其身份验证凭据。

要打开 DDP 控制台，请从*桌面*双击 **DDP 控制台**图标。

DDP 控制台 启动时，主页将显示 Security Tools 应用程序：

- 加密状态
- 注册
- Password Manager

要首次设置凭据，请选择 " 注册 " 磁贴上的**入门**链接。向导将引导您完成简短的注册过程。有关更多信息，请参阅首次注册凭据。

导航

要访问应用程序，请单击相应的磁贴。

标题栏

要从某个应用程序内返回主页，请单击标题栏左角该活动应用程序名称旁边的返回箭头。

要直接导航至另一个应用程序，请单击活动应用程序名称旁边的向下箭头，然后选择应用程序。

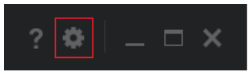
要最小化、最大化或关闭 DDP 控制台，请单击标题栏右角中的相应图标。

要在最小化 DDP 控制台后还原，请双击其系统托盘图标。

要打开 " 帮助 "，请单击标题栏上的 ?。

DDP 控制台详细信息

要查看关于 DDP 控制台、策略、运行服务和日志的详细信息，请单击标题栏左侧的齿轮图标。管理员提供技术支持时可能需要了解此信息。



从菜单中选择一个菜单项。

菜单项	用途
关于	包含版本和版权信息。
显示信息	包含以下信息： • 产品版本和日期信息 • 此计算机上的 DDP 控制台是由企业管理还是由本地管理员管理 • 操作系统的版本号、 BIOS、主板和可信平台模块 (TPM)。
MS 信息	运行 Microsoft Windows System Information 公用程序，以显示关于硬件、组件以及软件环境的详细信息。
复制信息	将所有系统信息复制到剪贴板，再粘贴到发送给管理员或 Dell ProSupport 的电子邮件中。
反馈	显示供您向 Dell 提供此产品相关反馈的表单。
策略	显示应用于此计算机的策略层次。
服务	显示正在运行的服务的详细信息。
支持	连接至 Dell ProSupport 网站。
日志	显示所记录事件的详细列表，用于故障排除。

3

加密状态

“ 加密 ” 页面显示计算机的加密状态。如果磁盘、驱动器或分区未加密，其状态将为*无保护*。已加密驱动器或分区的状态显示为*已保护*。

要更新加密状态，请右键单击相应的磁盘、驱动器或分区，然后选择**刷新**。

4

注册

“ 注册 ” 工具可供您根据管理员设置的策略来注册、修改或检查注册状态。

在您首次通过 DDP 控制台注册凭据时，向导将引导您注册密码更改、恢复问题、指纹、移动设备和智能卡。根据策略，可以注册或跳过各个凭据。初始注册后，可以单击 “ 注册 ” 磁贴以添加或修改凭据。

首次注册凭据

要首次注册凭据：

1. 在 DD 欢 P 控制台主页中，单击 “ 注册 ” 磁贴上的**入门**链接。
2. 在 “ 迎 ” 页面中，单击**下一步**。
3. 在 “ 需要身份验证 ” 对话框中，使用您的 Windows 密码登录，然后单击**确定**。
4. 在密码页面，如要更改您的 Windows 密码，请输入新密码并进行确认，然后单击**下一步**。

   要跳过更改密码，请单击**跳过**。如果您不想注册凭据，向导将允许您跳过。要返回到一个页面，则单击**后退**。
5. 按照每个页面上的说明操作，并单击相应的按钮：**下一步**、**跳过**或**后退**。
6. 在 “ 摘要 ” 页面，确认注册的凭据，并在完成注册时单击**应用**。

   要返回凭据注册页面进行更改，请单击**后退**直至到达您要更改的页面。

有关注册凭据或更改凭据的详细信息，请参阅添加、修改或查看注册。

添加、修改或查看注册

要添加、修改或查看注册，请单击**注册**磁贴。

左侧窗格中的选项卡列出了可用的注册。此部分内容因您的平台或硬件类型而异。

“ 状态 ” 页面显示所支持的凭据、凭据策略设置 （“ 必需 ” 或 “ 不适用 ”） 及其注册状态。从该页面，用户可根据管理员设置的策略管理其注册：

- 要首次注册凭据，请在该凭据所在的行单击**注册**。
- 要删除已注册的现有凭据，请单击**删除**。
- 如果策略不允许您注册或修改您自己的凭据，“ 状态 ” 页面上的**注册**和**删除**链接将处于非活动状态。
- 要更改现有注册，请单击左侧窗格中的相应选项卡。

  如果策略不允许注册或修改凭据，凭据注册页面将显示消息：“ 策略不允许修改凭据。 ”

密码

要更改 Windows 密码，请执行以下操作：

1. 单击**密码**选项卡。
2. 输入当前 Windows 密码。
3. 输入新密码，并再次输入以进行确认，然后单击**更改**。

   密码更改将立即生效。

4 在“成功注册”对话框中，单击**确定**。

注：只能在 DDP 控制台 中更改 Windows 密码，不能在 Windows 中更改。如果在 DDP 控制台 之外更改 Windows 密码，将发生密码不匹配的情况，需要执行恢复操作。

恢复问题

“恢复问题”页面可用于创建、删除或更改您的恢复问题及回答。恢复问题为您在密码过期或忘记密码等情况下访问 Windows 帐户提供一种问答式的方法。

注：恢复问题只用于恢复对计算机的访问。恢复问题及回答不能用于登录。

如果您以前未注册恢复问题：

1 单击**恢复问题**选项卡。

2 从预定义问题列表中选择，然后输入回答并进行确认。

3 单击**注册**。

注：单击重设按钮，以清除此页面上的选择并重新开始。

已注册恢复问题

如果已注册恢复问题，可删除或重新注册您的恢复问题。

1 单击**恢复问题**选项卡。

2 单击相应按钮：

- 要完全移除恢复问题，请单击**删除**。
- 要重新定义恢复问题及回答，请单击**重新注册**。

指纹

注：要使用这项功能，您的计算机必须具备指纹读取器。

要注册指纹，请按照以下说明操作：

1 单击**指纹**选项卡。

2 在“指纹”页面，单击要注册的手指。

3 根据屏幕说明注册指纹。

注：必须将手指成功扫描四次才能进行注册。完成指纹注册所需的扫描次数取决于每次扫描的质量。管理员定义了最小和最大指纹数。

4 单击后续的每个手指以进行扫描，直至您注册完策略所需的最小指纹数。

如果您尚未注册最小指纹数，将显示一个对话框告知您。单击**确定**以继续。

5 完成所需数目的指纹扫描，然后单击**保存**。

要删除已扫描的指纹，在“指纹注册”页面上，单击突出显示的指纹以取消注册，单击**是**以确认删除，然后单击**保存**。

移动设备

移动设备注册提供一次性密码 (OTP) 功能。通过 OTP，用户可使用与计算机配对的移动设备上的 Security Tools Mobile 应用生成的密码登录 Windows。如果策略允许， OTP 功能也可用于在密码过期或忘记密码时恢复对计算机的访问。

注： 如果 DDP 控制台中未显示 " 移动设备 " 选项卡，表明您的计算机配置不支持移动设备，或者管理员设置的策略不允许移动设备。

注： 策略设置决定 OTP 功能的用途 - 用于登录，或用于在密码过期或忘记密码时恢复对计算机的访问。 OTP 不能同时用于登录和恢复。

要使用 OTP 功能，必须注册或将您的移动设备与计算机配对。在一台拥有多个用户的计算机上，每个用户可对该计算机注册一个移动设备。移动设备可向多台计算机注册。

如果已注册了一个设备，注册新设备将自动取消以前设备的配对。

在 DDP 控制台上：

1. 在 DDP 控制台的 " 注册 " 页面中，单击**移动设备**选项卡。
2. 单击右上方的**注册**。

   " 注册一次性密码 " 页面随即打开。
3. 如果这是要配对的第一台计算机，请选择**是**。
   a. 在移动设备上，从您的应用商店下载 Dell Data Protection | Security Tools Mobile 应用。
   b. 在计算机上，单击**下一步**。

设置 Security Tools Mobile

1. 打开 Security Tools Mobile 应用。
2. 创建一个 PIN 并输入此 PIN，以访问 Security Tools Mobile 应用。

   注： 移动设备未锁定时，根据策略可能要求提供 PIN。如果您不使用 PIN 来解锁移动设备，则需要一个 PIN 来访问 Security Tools Mobile 应用。
3. 选择**注册计算机**。（如果需要，点击移动设备屏幕的左上角以访问命令。）

   此时移动设备上将显示一个代码。代码长度和字母数字组合基于管理员设置的策略。

配对移动设备和计算机

1. 在计算机上，在 DDP 控制台的 " 移动代码 " 页面中：
   a. 在字段中输入移动设备上的代码。
   b. 单击**下一步**。
   c. 在 " 配对设备 " 页面，选择以下的一项：

      QR 二维码 - 将显示 QR 二维码。

      或

      手动输入 - 将显示 24 位配对代码。
2. 在移动设备上：
   a. 点击**配对设备**。
   b. 选择您在计算机上选择的相同配对选项 （**扫描 QR 二维码**或**手动输入**）。
   c. 选择一项：

- 对于 QR **二维码**，将移动设备置于计算机屏幕前面，以扫描 QR 二维码。
  记下移动设备上显示的数字验证码，然后点击**下一步**。

注：如果显示*扫描遇到问题？*栏，请重试，或选择**手动输入**。

- 对于**手动输入**，请输入计算机上的 24 位配对代码，然后点击**完成**。
  记下移动设备上显示的数字验证码，然后点击**下一步**。

3 在计算机上的 DDP 控制台中：

a 单击**下一步**。

b 输入移动设备上显示的验证码，然后单击**下一步**。

c 或者您也可以修改移动设备的名称。

d 单击**应用**。
设备配对完成。

4 在移动设备上：

a 点击**继续**。

b 或者，修改计算机的名称，然后点击**完成**。

c 点击**完成**。

注册另一台移动设备

注册新设备将自动取消以前设备的配对。取消配对无需执行单独的操作。

取消计算机与移动设备配对

要取消计算机与移动设备配对并且不注册另一台设备，请选择以下一项：

- 在 DDP 控制台上：在“注册状态”页面上的“移动设备”凭据旁，单击**删除**。
- 在移动设备上：
  1 运行 Security Tools Mobile 应用。
  2 点击左上角的菜单栏以打开抽屉。
  3 点击**移除计算机**。
  4 选择要取消配对的计算机。
  5 选择**移除** (Android) 或点击**完成** (iOS)。
  此时会显示确认消息。
  6 选择**全部移除**以从您的设备上移除所有已注册的计算机。
  当您要移除多个计算机以及仅移除已配对的计算机时，会显示“全部移除”选项。
  - 选择**恢复默认设置**以移除已注册的计算机并移除 PIN。如果您恢复默认设置，所有已注册的计算机以及您用于访问 Security Tools Mobile 应用的 PIN 都将被移除。
  - 选择**取消**以保留计算机注册。

使用一次性密码登录

注： OTP 身份验证仅可用于 Windows 登录。

OTP 可用于恢复，以在您被锁定的情况下重新获得对计算机的访问，或者用于 Windows 登录。但不能同时用于两种用途。

如果策略允许，并且登录屏幕上显示有 OTP 符号  ，则可使用 OTP 登录 Windows。

要使用 OTP 登录：

1. 在计算机的 Windows 登录屏幕上，选择 OTP 图标  。
2. 在移动设备上，打开 Security Tools Mobile 应用并输入 PIN。
3. 选择您要访问的计算机。

   如果移动设备上未显示计算机名称，可能发生了以下一种情况：

   - 移动设备未注册或未与您尝试访问的计算机配对。
   - 如果您有多个 Windows 用户帐户，则可能是您尝试访问的计算机上未安装 Security Tools，或者您尝试登录的用户帐户不是配对计算机和移动设备时所使用的用户帐户。
4. 点击**一次性密码**。

   此时移动设备屏幕上将显示一个密码。

   注： 如果需要，可单击“刷新”符号  以获取新代码。刷新前两个 OTP 后，将延迟三十秒才生成另一个 OTP。计算机和移动设备必须同步，二者才能同时识别同一个密码。如尝试快速相继生成密码，将导致计算机和移动设备不同步以及 OTP 功能失效。如发生该问题，请等待三十秒以使两个设备恢复同步，然后再重试。
5. 在计算机的 Windows 登录屏幕上，键入移动设备上显示的密码并按 **Enter** 键。

   如果您使用了 OTP 进行恢复，在获得对计算机的访问后，请根据屏幕说明重设密码。

Security Tools Mobile 管理任务

这些任务使用移动设备上的 Security Tools Mobile 应用执行。

重设 Security Tools Mobile 应用的 PIN

要重设 Security Tools Mobile 应用的 PIN：

1. 点击右上方的菜单选项。
2. 选择**重设 Pin**。
3. 输入新 PIN 并进行确认。

卸载 Security Tools Mobile 应用

在移动设备上：

1. 取消设备与计算机配对。
2. 删除或卸载 Security Tools Mobile 应用，如同您通常从移动设备中删除应用一样。

智能卡

注：要使用这项功能，您的计算机必须具备智能卡读卡器。

要注册智能卡，请按照以下说明操作：

1. 单击**智能卡**选项卡。
2. 注册智能卡，根据卡的类型：
   - 将智能卡插入读卡器。
   - 对于非接触式卡，应握住卡并将卡放到读卡器上或读卡器附近。
3. 在检测到智能卡时，将显示绿色的复选框和*注册卡*。选择**注册卡**。
4. 在“成功注册”对话框中，单击**确定**。

要取消注册与该用户关联的所有智能卡，请在“智能卡注册”页面上选择“**从您的帐户移除已注册的卡**”。

5

Password Manager

Password Manager 可供您自动登录网站、 Windows 程序和网络资源，以及在单一工具中管理多个登录凭据。Password Manager 还为用户提供通过此应用程序更改其登录密码的功能，确保 Password Manager 所维护的密码与目标资源的密码保持同步。

Password Manager 支持 Internet Explorer 和 Mozilla Firefox。 Password Manager 不支持 Microsoft 帐户 （以前的 Windows Live ID）。

注：如果在 Firefox 上运行 Password Manager，必须安装和注册 Password Manager 扩展项。有关在 Mozilla Firefox 中安装扩展项的说明，请参阅 https://support.mozilla.org/。

注：Mozilla Firefox 中的 Password Manager 图标 （包括设定前和设定后的图标）的用法与其在 Microsoft Internet Explorer 中的用法不同：

- Password Manager 图标的双击功能不可用。
- 在下拉上下文菜单中，默认操作没有以粗体显示。
- 如果页面包含多个登录窗体，则会看到多个 Password Manager 图标。

注：由于 Web 登录页面的结构不断变化， Password Manager 可能无法始终为所有网站都提供支持。

Password Manager 入门

Password Manager 将在您操作时收集并存储您的登录凭据。您可以在安装 Security Tools 之后立即开始使用 Password Manager。当您在登录页面中输入凭据时，Password Manager 将检测登录形式，并让您选择是否要 Password Manager 保存凭据。

您有三个选择：

- 单击**保存登录**可将您的登录凭据存储在 Password Manager 中。
- 如果您**不**希望保存登录，则每次您登录该网站或程序时，都会再次提示您保存登录凭据。如果您不希望收到提示，请选择**对此站点不再提示**。这样将在 " 网站排除 " 列表中创建一条记录。详情请参阅排除网站。
- 如果您不希望保存凭据，请单击**不保存登录**。

如果您以前保存了某个网站或程序的凭据，但您输入了不同的用户名或密码时，此对话框也将显示。对于新用户名，如果您选择**保存登录**，将存储一组新的凭据。对于以前保存的用户名和新密码，如果您选择**保存登录**，初始凭据将被新密码更新。

管理登录

登录管理器简化并集中管理您对网站、 Windows 程序和网络资源的所有登录。

要打开登录管理器：

1. 在 DDP 控制台主页上，单击 **Password Manager** 磁贴。
2. 单击**登录管理器**选项卡。

您可以添加登录和类别，并对其进行排序和筛选：

- 添加登录 - 允许您添加一组新的登录凭据。根据策略，您可能需要输入存储在 Security Tools 中的凭据才能添加登录。

- 添加类别 - 允许您添加一种新的类别 （例如电子邮件、存储、新闻、企业资源、社交媒体）以用于排序和筛选。

排序：按帐户、用户名或类别对登录进行排序。单击列标题可按该列排序。

筛选：从*视图*列表中选择一种类别，可隐藏除选定类别登录以外的所有登录。要移除筛选器，请选择*全部*。

您可以管理登录：

- 启动 - 根据用户设置打开网站或程序，并提交登录凭据。
- 编辑 - 允许您更改网站或程序的存储的登录数据。
- 删除 - 允许您从 Password Manager 移除已存储的登录数据。
- 添加 - 允许您添加新的登录、类别或新的登录数据。

添加类别

在添加登录前创建类别 （例如电子邮件、存储、新闻、企业资源和社交媒体），以便在创建登录时对登录进行分类。然后您便可按类别对登录进行排序和筛选。

要添加类别，请在 " 登录管理器 " 页面上单击**添加类别**，输入类别名称，然后单击**保存**。

添加登录

1. 在 " 登录管理器 " 页面中，单击**添加登录**。

   根据策略，添加登录可能需要进行身份验证。
2. 打开要登录的网站或程序。
3. 在 " 添加登录 " 对话框中，单击**继续**。
4. 在接下来的对话框中，输入以下信息：
   - **类别** - 为您存储的网站或程序的登录选择一种类别。如果尚未添加类别，此列表将为空。
   - **帐户名称** - 将此字段保持不变以接受预填的名称，或键入网站或程序的名称。
   - **未检测标题** - 这些字段是 Password Manager 在登录页面上检测到的、您在其中输入登录信息的字段。这些字段通常包含用户名或电子邮件和密码。
5. 如果字段名称显示为 " 未检测标题 "，或者将不当的字段作为登录字段包含进来，请单击**更多字段**按钮以编辑字段名称或移除字段。
6. 在 " 更多字段 " 对话框中，单击**未检测标题**，并为每个字段输入正确的字段名称。

   显示 " 更多字段 " 对话框时，" 添加登录 " 对话框中的活动字段将突出显示，以帮助您重命名这些字段。

   如果某个字段对于登录是非必要的，可清除其复选框以将其排除在登录信息之外。
7. 要保存更改，请单击**确定**。
8. 在 " 添加登录 " 对话框中，填写登录必填字段。

注：由于您存储的是现有登录，因此只能通过网站或程序的 " 更改密码 " 功能更改密码。

9. 如果希望 Password Manager 自动填充和提交登录信息，请选择**自动提交登录数据**。
10. 单击**保存**。

    此网站或程序的登录将显示在 " 登录管理器 " 页面上。

导入凭据

您可以将存储在 Web 浏览器中的凭据导入 Password Manager。

1 在 Password Manager 工具中，选择**导入凭据**。

2 选择要导入的浏览器，然后单击**扫描**。

3 根据提示输入所选浏览器的密码。

注：如果导入后未导入密码，请检查以确定浏览器是否存储了要导入的数据。如果您使用的是 Firefox，请登录以进行同步。然后再次尝试导入凭据。

图标上下文菜单

当您访问网站或程序时，会显示 Password Manager 图标。

表示该登录表单可进行设定。

如果未显示 ，则表明该登录表单已进行设定。双击此图标以登录到程序或网站。

单击图标后，上下文菜单将根据该登录表单是已设定还是未设定来显示不同选项。

如果当前登录字段尚未进行设定，上下文菜单将显示以下选项：

添加到 Password Manager -	*打开“添加登录”对话框。*
图标设置	可供用户配置 Password Manager 图标在可培训登录页面上的显示。
打开 Password Manager	启动 *Password Manager Administration* 工具并打开“登录管理器”页面。
帮助	打开联机帮助。

如果当前登录字段已设定，上下文菜单将显示以下选项：

填充登录数据	根据您在设定登录表单时的选择，将自动登录，或者填充用户名和密码字段以便您提交登录数据。
编辑登录	打开“编辑登录”对话框。
添加登录	打开“添加登录”对话框。
打开 Password Manager	打开“登录管理器”页面。
帮助	打开联机帮助。

如果登录表单未显示 Password Manager 图标，请关闭浏览器的密码保存功能：

- 在 Mozilla Firefox 中：菜单图标 > 选项 > 安全性 > 清除**记住站点密码**复选框
- 在 Internet Explorer 中：齿轮图标 > Internet 选项 >“内容”选项卡 > 自动完成设置 > 清除**表单上的用户名和密码**复选框

登录到已设定的登录页面

打开网站或程序登录时， Password Manager 将检测此页面是否已设定。如果已设定，登录区域将显示 Password Manager 图标。如果未设定，将显示 Password Manager 图标 - 除非已禁用未设定表单提示。

要登录，请从以下选择一种方法：

- 扫描已注册的凭据。如果您注册了指纹或智能卡，可用已注册的指纹触摸指纹读取器，或向读卡器出示一张已注册的卡。
- 单击 Password Manager 图标，然后从上下文菜单中选择**填写登录数据**。
- 按 Password Manager 热键组合：**Ctrl+Win+H**。 Password Manager 将在弹出窗口中为您展示已设定的站点，以供您快速启动其中的一个站点。

注：您可以通过 DDP 控制台 > Password Manager > 设置，来更改热键组合。

如果该站点或程序存储了多个登录，将提示您选择要使用的帐户。

Web 域支持

如果您设定了特定 Web 域的登录页面，但希望从不同的登录页面访问该 Web 域上的帐户，请导航至新登录页面。然后将提示您使用现有登录或向 Password Manager 中添加新的登录。

- 如果单击*使用登录*，您将登录到以前创建的帐户。下次您从新登录页面访问此帐户时，将自动登录到以前创建的帐户。
- 如果单击*添加登录*，将显示添加登录对话框。

填充 Windows 凭据

有些程序允许使用 Windows 凭据登录。

您无需键入用户名和密码，只需从*添加登录*和*编辑登录*对话框中的可用下拉菜单中选择 Windows 凭据。

对于用户名，请选择以下类型：

- Windows 用户名
- Windows 用户主要名称
- Windows 域\用户名
- Windows 域

对于密码，请使用您的 Windows 密码。

这些选项不能进行修改。

使用旧密码

在 Password Manager 中更改了密码，但之后程序拒绝新密码的情况有可能发生。如果发生这种情况，程序将允许您使用以前的密码 （以前在此登录页面中输入过的密码）而不是最新的密码。

选择**密码历史**。在身份验证后，系统会提示您从 " 密码历史 " 列表中选择一个旧密码。该列表包含 7 个密码。

排除网站

要禁止网站受 Password Manager 管理，请单击**网站排除**选项卡。

排除的网站具有以下特征：

- 不调用 Password Manager 图标。
- 不自动登录用户。
- 不显示密码提示。

要将新网站添加至排除列表：

1. 单击**网站排除**选项卡。
2. 单击**添加网站**。
3. 输入要排除的网站的 URL。
4. 单击**保存**。

排除某个网站后，该网站不受 Password Manager 管理。从 " 网站排除 " 列表中删除该网站，即可撤消排除。要从排除列表中移除某个网站：单击 ✕。

添加多个网站后，您可以：

- 要按网站对列表进行升序或降序排序，请单击 " 网站 " 列标题。
- 要在列表中搜索网站，请在搜索字段输入其部分 URL。此列表将按您的输入进行筛选。

禁用设定登录表单提示

您可以保持已设定的现有登录，但禁用设定新登录表单提示。

要禁用新登录提示：

1. 打开 DDP 控制台。
2. 单击 **Password Manager** 磁贴。
3. 单击**设置**选项卡。
4. 清除**在登录屏幕上时提示添加登录**复选框。

备份和还原 Password Manager 凭据

Password Manager 可安全备份由 Password Manager 管理的登录数据。该数据可还原到任何一台受 Password Manager 保护的计算机上。

注：备份的 Password Manager 数据不包含操作系统或 预引导身份验证 (PBA) 登录凭据或凭据特定的信息 （例如指纹）。

备份凭据

要备份凭据：

1. 单击**备份凭据**选项卡以设定备份过程。
2. 单击**浏览**并导航至所需的备份位置。

   如果试图将数据备份到本地驱动器，将建议把数据备份到可移动存储或网络驱动器上。
3. 输入并确认密码。如果以后必须还原这些备份凭据，必须使用此密码。
4. 单击**备份**。
5. 输入您的 Windows 密码。
6. 在 " 成功 " 对话框中，单击**确定**。

注：要查看执行的备份操作的文本日志，请单击 并选择**日志**。

还原凭据

备份位置必须可用才能还原凭据。

要还原凭据：

1. 单击**还原凭据**选项卡。
2. 单击**浏览**以导航至备份文件，然后输入此文件的密码。
3. 单击**还原**。

警告：还原 Password Manager 数据将覆盖现有数据。创建备份后添加的登录及其他数据将丢失。

4. 单击**下一步**。

注：要查看还原操作的文本日志，请单击标题栏中的 图标，然后选择**日志**。

词汇表

可信平台模块 (TPM) - TPM 是一块安全芯片，它有三项主要功能：安全存储、测量和证明。DDP|E 将 TPM 用于其安全存储功能。TPM 也可为 DDP|E 软件保管库提供加密容器，以及用于保护 DDP|E HCA 加密密钥。Dell 建议您配置 TPM。DDP|E HCA、BitLocker Manager 和一次性密码功能需要使用 TPM。

凭据 - 凭据是用于证明个人身份的信息，例如个人指纹或其 Windows 密码。

一次性密码 (OTP) - 仅可使用一次并且只在有限的时段内有效的密码。OTP 要求 TPM 已存在、已启用且已有归属。要启用 OTP，需要使用 DDP 控制台和 Security Tools Mobile 应用，将移动设备与计算机配对。Security Tools Mobile 应用在移动设备上生成密码，此密码用于从 Windows 登录屏幕登录到计算机。根据策略，如果 OTP 尚未用于登录该计算机，则在密码过期或忘记密码时可使用 OTP 功能恢复对该计算机的访问。OTP 功能可用于身份验证或用于恢复，但不能同时用于这两项用途。OTP 的安全性超过其他一些身份验证方法，因为所生成的密码只能使用一次并且会在短时间内过期。

已保护 - 对于自加密驱动器 (SED)，在激活 SED 并且部署预引导身份验证 (PBA) 后，计算机即受到保护。

预引导身份验证 (PBA) - 预引导身份验证是对 BIOS 或引导固件的扩展，在操作系统之外作为可信身份验证层，保证安全且防篡改的环境。PBA 防止读取硬盘中的任何内容 （如操作系统），直至用户确认其具备正确凭据。

自加密驱动器 (SED) - 具有内置加密机制的硬盘驱动器，自动对存储在介质上的所有数据进行加密，并自动解密脱离介质的所有数据。这种加密类型对于用户完全透明。


0XXXXXA0X