حماية البيانات من Dell

أدوات الأمان لنظام Android

دليل المسؤول

المحتويات

نظرة عامة على أدوات الأمان لنظام Android

تعد Dell Data Protection | Security Tools (DDP|ST) للأجهزة التي تعمل بنظام Android هي حل تأمين النقطة النهائية المخصص لاستخدام الشركات فيما يتعلق بأجهزة الكمبيوتر اللوحي المدعومة من Dell.

مبدئياً، تكون أجهزة الكمبيوتر اللوحي من Dell في وضع المستهلك. لتمكين ميزات DDP|ST for Android واستخدامها، يجب عليك تبديل وضع جهاز الكمبيوتر اللوحي إلى الوضع التجاري. لمزيد من المعلومات، راجع تنزيل وتشغيل تطبيق DDP|ST Agent.

المتطلبات

أجهزة الكمبيوتر اللوحي

يسرد هذا الجدول أجهزة الكمبيوتر اللوحي المدعومة.

أجهزة الكمبيوتر اللوحي
• Dell Venue 8 7840
• Dell Venue 10 7040

أنظمة تشغيل الأجهزة المحمولة

أدوات الأمان لنظام Android

يسرد هذا الجدول أنظمة التشغيل المدعومة لأجهزة الكمبيوتر اللوحي المقدمة من Dell.

أنظمة التشغيل للأجهزة التي تعمل بنظام Android
• 5.0 - 5.1 Lollipop

أدوات الأمان المقدمة من Dell للأجهزة المحمولة

يسرد هذا الجدول أنظمة التشغيل المدعومة فيما يتعلق بأدوات الأمان في حالة إقران أجهزة الكمبيوتر اللوحي المقدمة من Dell بجهاز محمول آخر.

أنظمة التشغيل للأجهزة التي تعمل بنظام Android
• 4.0 - 4.0.4 Ice Cream Sandwich
• 4.1 - 4.3.1 Jelly Bean
• 4.4 - 4.4.4 KitKat
• 5.0 - 5.1 Lollipop
أنظمة التشغيل iOS
• iOS 7.x
• iOS 8.x
أنظمة التشغيل Windows
• Windows 8.1 Phone
• Windows 10 Mobile

السياسات

للحصول على معلومات مفصلة عن سياسات DDP|ST for Android، ارجع إلى *مساعدة المسؤول "Admin Help"*، المتاحة على وحدة التحكم بالإدارة عن بعد. كما يتم عرض وصف السياسات أيضاً كتلميحات الأدوات في وحدة التحكم بالإدارة عن بعد.

يمكنك تمكين سياسات DDP|ST for Android على المستويات التالية:

- المؤسسات
- المجال
- مجموعات المستخدم
- المستخدمون

مهام المسؤول

تمكين الحماية على خادم حماية البيانات من "Dell "DDP

لتمكين الحماية على Dell Enterprise Server أو خادم حماية البيانات من Dell الخاص بالمؤسسات "DDP Enterprise Server" - النسخة الافتراضية "VE" لأجهزة الكمبيوتر اللوحي DDP|ST، قم بفتح وحدة التحكم بالإدارة عن بعد وتأكد من أن سياسة *تمكين الحماية* على الأجهزة التي تعمل بنظام Android تم ضبطها على وضع **متحقق** (كوضع افتراضي). حيث يمثل ذلك السياسة الرئيسية لكل سياسات DDP|ST for Android الأخرى:

- متحقق – يقوم خادم DDP بإدارة تطبيقات DDP الموجودة على جهاز الكمبيوتر اللوحي من Dell.
- غير متحقق – لا يقوم خادم DDP بإدارة تطبيقات DDP الموجودة على جهاز الكمبيوتر اللوحي من Dell. وبالتالي تصبح إعدادات سياسة DDP|ST for Android الأخرى غير متعلقة بالتطبيقات.

إعداد حسابات المستخدم على DDP Server

لإعداد حسابات المستخدم على DDP Server:

1. بصفتك مسؤول بشركة Dell، قم بتسجيل الدخول إلى وحدة التحكم بالإدارة عن بعد.
2. في الجزء الأيسر، انقر فوق **حماية وإدارة > المجالات**.
3. انقر فوق رمز **الأعضاء** الخاص بالمجال الذي تريد إضافة المستخدم إليه.
4. انقر فوق **إضافة مستخدمين**.
5. قم بإدخال عامل تصفية للبحث عن اسم المستخدم من خلال الاسم الشائع *Common Name*، أو الاسم الرئيسي العالمي *Universal Principal Name*, أو اسم *sAMAccountName*. حرف البدل هو *.

   يجب تعريف الاسم الشائع Common Name، والاسم الرئيسي العالمي Universal Principal Name، واسم sAMAccountName في خادم دليل المؤسسة لكل مستخدم. إذا كان المستخدم عضواً في المجال أو المجموعة ولكنه لا يظهر في قائمة أعضاء المجال أو المجموعة في وحدة التحكم بالإدارة عن بعد، تأكد من أنه تم تعريف كل الأسماء الثلاث بطريقة صحيحة لكل مستخدم في خادم دليل المؤسسة.

   سيقوم الاستعلام بالبحث تلقائياً عن الاسم الشائع ثم الاسم الرئيسي العالمي "UPN" ثم اسم sAMAccount حتى يتم العثور على نتائج مطابقة.
6. قم بتحديد المستخدمين من قائمة مستخدم الدليل لإضافتهم إلى المجال. استخدم **<Shift><click>** أو **<Ctrl><click>** لتحديد عدة مستخدمين.
7. انقر فوق **إضافة المحدد "Add Selected"**.

إخطار المستخدمين

بعد أن يتم تعيين حسابات المستخدم، يجب على المستخدمين تنزيل تطبيق DDP|ST Agent ثم تنشيط التطبيق على خلفية خادم DDP.

- أخطر المستخدمين عندما يتم تعيين حساباتهم.
- أخبر المستخدمين إذا ما كان يجب عليهم تنزيل تطبيق DDP|ST Agent من Google Play Store أو من موقع آخر.
- أخبرهم ببيانات الاعتماد التي يجب استخدامها لتسجيل الدخول.
- قم بإرسال عنوان خادم DDP لهم لاستخدامه لتسجيل الدخول.
- إذا قمت بتمكين DDP|ST Password Manager، فقم بإخبار المستخدمين عن متطلبات طول كلمة المرور الرئيسية والأحرف.

تمكين استعادة كلمة المرور الصالحة لمرة واحدة "OTP"

تسمح هذه الميزة للمستخدم الذي ينسى كلمة المرور الخاصة به بالحصول على كلمة المرور الصالحة لمرة واحدة لإلغاء قفل جهاز الكمبيوتر اللوحي من Dell ثم إعادة تعيين كلمة المرور. لتمكين هذه الميزة، يجب أن يقترن جهاز الكمبيوتر اللوحي بجهاز هاتف ذكي أو هاتف محمول يقوم بتشغيل تطبيق Dell Security Tools.

تعد سياسة *تمكين استعادة كلمة المرور الصالحة لمرة واحدة "OTP"* السياسة الرئيسية لكل سياسات كلمة المرور الصالحة لمرة واحدة. تقوم شاشة تسجيل الدخول بالتحقق من السياسة قبل السماح باستعادة كلمة المرور الصالحة لمرة واحدة "OTP" حتى في حالة اقتران جهاز الكمبيوتر اللوحي.

لتمكين استعادة كلمة المرور الصالحة لمرة واحدة:

1 في وحدة التحكم بالإدارة عن بعد، قم بضبط سياسة *تمكين استعادة كلمة المرور الصالحة لمرة واحدة "OTP"* على وضع **متحقق**.

- متحقق – يتم تمكين ميزة استعادة كلمة المرور الصالحة لمرة واحدة وتسمح للمستخدم باستخدام جهاز هاتف محمول مقترن لإنشاء كلمات المرور الصالحة لمرة واحدة لإلغاء قفل الحساب الخاص به في حالة فقدان كلمة المرور الخاصة بالحساب.
- غير متحقق (وضع افتراضي) – لن يتمكن المستخدمين من استخدام استعادة كلمة المرور مرة واحدة "OTP" بغض النظر عن القيم الأخرى لسياسة استعادة كلمة المرور مرة واحدة "OTP".

ملاحظة: عندما يقوم المستخدم بفتح تطبيق DDP|ST Mobile Pairing لإقران الأجهزة ببعضها، يقوم التطبيق أولاً بالتحقق من تمكين استعادة كلمة المرور مرة واحدة "OTP". إذا تم ضبط سياسة تمكين استعادة كلمة المرور الصالحة لمرة واحدة "OTP" على وضع غير متحقق أو تم تغييرها إلى وضع غير متحقق بعدما قام المستخدمين بإقران أجهزة الكمبيوتر اللوحي الخاصة بهم بالأجهزة الأخرى، يكون الرمز DDP|ST Mobile Pairing غير مرئي على أجهزة الكمبيوتر اللوحي الخاصة بالمستخدمين.

2 قم بضبط القيمة *للحد الأقصى من محاولات استعادة كلمة المرور مرة واحدة "OTP"*. تتمثل الخيارات المتاحة في النطاق *من 5 إلى 10* مع وجود قيمة افتراضية تتمثل في *5*.

3 قم بضبط قيمة *الحد الأقصى لفشل محاولات إجراء الاستعادة*.

4 الخيار الافتراضي هو عدم *الاقتران*، مما يعني إلغاء الاقتران بين جهاز الكمبيوتر اللوحي والهاتف المحمول وإلغاء تمكين استعادة كلمة المرور الصالحة لمرة واحدة.

5 التزم بالسياسات.

تهيئة DDP|ST Password Manager

يسمح تطبيق DDP|ST Password Manager للمستخدمين بإدارة كلمات المرور بشكل آمن. يمكن للمستخدمين تخزين كل كلمات المرور الخاصة بهم داخل التطبيق، مما يحمي كلمات المرور باستخدام المفتاح الرئيسي. يمكن أن يتم إلغاء قفل المفتاح الرئيسي فقط باستخدام كلمة المرور الرئيسية. يجب أن يتذكر المستخدمون كلمة المرور الرئيسية الخاصة بهم فقط للوصول إلى كلمات المرور الأخرى التي تم تخزينها في DDP|ST Password Manager.

تمكين DDP|ST Password Manager

لتمكين إدارة كلمات المرور Password Manager في وحدة التحكم بالإدارة عن بعد، قم بضبط *تمكين سياسة Password Manager* سياسة على وضع **متحقق**. تلك هي السياسة الرئيسية لـ Password Manager.

- متحقق - يكون Password Manager متاحاً ويتم قبول بيانات اعتماد تسجيل الدخول الجديدة للمستخدم وتخزينها.
- غير متحقق (وضع افتراضي) - يكون Password Manager غير متاحاً بغض النظر عن القيم الخاصة بالسياسة الأخرى.

تعيين المتطلبات الخاصة برموز المرور الرئيسية لـ Password Manager

يمكنك تعيين رموز المرور الرئيسية لـ Password Manager عن طريق إعداد السياسات التالية:

1 قم بتحديد قيمة الحد *الأدنى لطول رمز المرور*:

- *من 0 إلى 18* حرفاً (حيث يكون العدد الافتراضي *8*)

2 قم بتحديد القيم الخاصة بسياسة الأحرف:

- *يُسمح باستخدام الأحرف البسيطة في رموز المرور*
  - متحقق (وضع افتراضي) – قد تحتوي رموز المرور على أحرف مكررة أو أحرف تصاعدية / تنازلية (مثل ABC أو 321).
  - غير متحقق – لا يُسمح برموز المرور البسيطة.
- *يجب استخدام الأحرف الأبجدية الرقمية في رموز المرور*
  - متحقق (وضع افتراضي) – يجب أن يتضمن رمز المرور مجموعة من الأحرف والأرقام.
  - غير متحقق – لا يتطلب استخدام الأحرف الأبجدية الرقمية في رمز المرور.
- *الحد الأدنى للأحرف المعقدة في رمز المرور*
  - *0-4* حرف (حيث يكون العدد الإفتراضي *1*)
  - الأحرف المعقدة هي الأحرف التي لا تمثل الأرقام أو الحروف (#$%&)

3 تأكد من إخطار المستخدمين النهائيين بمتطلبات رموز المرور الرئيسية التي قمت بتعيينها.

تحديد طول المدة الزمنية لعدم التنشيط

يمكنك تحديد عدد الدقائق التي يمكن أن يكون فيها الجهاز خاملاً (بدون إدخال المستخدم) قبل قفل Password Manager. بعد الوصول إلى هذا الحد، يتم قفل Password Manager ويجب على المستخدم إدخال رمز المرور الخاص به. قم بتعيين عدد من الدقائق يتراوح بين 1 إلى 60 دقيقة في سياسة *فترة عدم نشاط في قفل تطبيق Password Manager*. الوقت الافتراضي هو *5* دقائق.

استكشاف الأخطاء وإصلاحها

لا يمكنني تسجيل الدخول باستخدام عنوان خادم DDP أو لا أتمكن من الوصول إلى تطبيقات DDP|ST Agent.

راجع تعيين خيار قفل الشاشة على جهاز الكمبيوتر اللوحي.

تظهر رسالة خطأ: إن إمكانية تعدد المستخدمين الخاصة بـ Commercial Android غير مدعومة.

يتم حاليًا دعم حساب مالك الكمبيوتر اللوحي فقط من خلال Commercial Android.

لم يعد الكمبيوتر اللوحي لدي مقترناً بالجهاز الأصلي الخاص بي.

هل قمت بتسجيل جهاز جديد؟ يعمل ذلك على إلغاء الاقتران تلقائياً بالجهاز السابق.

لا يتم عرض تطبيقات DDP|ST Password Manager و DDP|ST Mobile Pairing مرةً أخرى.

هل قمت بالضغط على **إلغاء التثبيت** في تطبيق DDP|ST Agent؟ إذا كان الأمر كذلك، فسيتم تعطيل التطبيقين الآخرين ولن يتم عرضهما مرةً أخرى. ومع ذلك، لا تزال البيانات الخاصة بك موجودة. إذا قمت بتشغيل تطبيق **DDP|ST Agent** وتنشيطه على خلفية خادم DDP، سيتم عرض التطبيقات الأخرى وستتوفر البيانات الخاصة بك.

لقد قمت بالضغط على رمز DDP|ST Password Manager، ولكن لم يتم عرض أي شيء.

تحقق بالرجوع إلى المسؤول الخاص بك مما إذا تم تمكين استعادة كلمة المرور الصالحة لمرة واحدة بالنسبة لك. إن لم يكن كذلك، استفسر عما إذا كان ذلك خياراً متاحاً لك.

تجربة المستخدم النهائي

لاستخدام DDP|ST for Android، يجب عليك تحويل وضع الكمبيوتر اللوحي الخاص بك من Dell من وضع المستهلك إلى الوضع التجاري. وسوف يقوم المسؤول الذي تتعامل معه بالتالي:

- إخطارك بأنه تم إعداد حساب المستخدم الخاص بـ DDP|ST for Android لديك
- إخبارك ببيانات الاعتماد الخاصة بتسجيل الدخول
- إرسال عنوان خادم DDP الخاص بتسجيل الدخول
- إخبارك بمتطلبات طول كلمة مرور **Password Manager** الرئيسية والحروف اللازمة لها.

تعيين خيار قفل الشاشة على جهاز الكمبيوتر اللوحي

لتعزيز التأمين عند استخدام DDP|ST for Android، ينبغي عليك تعيين قفل الشاشة. قبل استخدام تطبيق DDP|ST Agent، انتقل إلى **الإعدادات** > **تأمين** > **قفل الشاشة** على جهاز الكمبيوتر اللوحي من Dell وقم بتعيين نمط، أو رمز PIN، أو كلمة مرور. وخلاف ذلك، لن تتمكن من الوصول إلى تطبيقات DDP|ST Agent.

تنزيل وتشغيل تطبيق DDP|ST Agent

لبدء الاستخدام:

1 قم بتنزيل تطبيق **DDP|ST Agent** على جهاز الكمبيوتر اللوحي  .

ملاحظة: ستخبرك المؤسسة لديك إذا ما كان يجب عليك تنزيل التطبيق من Google Play Store أو من موقع آخر.

2 في شاشة التطبيقات "APPS drawer" في جهاز الكمبيوتر اللوحي، اضغط على الرمز **DDP|ST Agent**.
يتم عرض شاشة Dell Data Protection | ST Agent.

3 اضغط على **موافق** للحصول على اتفاقية الترخيص.

4 أدخل عنوان خادم DDP.

5 أدخل الاسم الذي تستخدمه لتسجيل الدخول وكلمة المرور، وفقاً للمعلومات المقدمة من المسؤول لديك.

6 اضغط على **تسجيل الدخول**.
تم ضبط جهاز الكمبيوتر اللوحي الآن على الوضع التجاري، و يقوم DDP|ST Agent بعرض هذه التطبيقات:

- DDP|ST Password Manager
- DDP|ST Mobile Pairing

تسجيل الأجهزة وإقرانها

يتيح لك إقران جهاز الكمبيوتر اللوحي من Dell بهاتف محمول آخر استعادة كلمة المرور في حالة نسيانك لها.

- على جهاز الكمبيوتر اللوحي الخاص بك من Dell، تأكد من تنزيل وتشغيل تطبيق DDP|ST Agent.
- على الجهاز المحمول الآخر أو الهاتف الذكي، قم بتثبيت وفتح تطبيق الهاتف **المحمول Dell Security Tools**  .

ملاحظة: ستخبرك المؤسسة لديك إذا ما كان يجب عليك تنزيل التطبيق من Google Play Store أو من موقع آخر.

على الجهاز المحمول أو الهاتف الذكي

1 عليك القيام بإحدى الخطوات التالية:

- إذا قمت بتثبيت تطبيق **Dell Security Tools** للتو، اضغط على **تخطي**، ثم اضغط على **بدء التشغيل**. ثم قم بإنشاء رمز PIN وتأكيده.
- إذا قمت بتثبيته سابقاً، قم بتشغيل تطبيق **Dell Security Tools**، ثم إدخال رمز PIN الخاص بك، واضغط على **تسجيل الدخول**.

2 في أسفل الشاشة التالية، اضغط على تسجيل جهاز الكمبيوتر. (يجب تنفيذ تلك الخطوات أيضاً عند **تسجيل جهاز كمبيوتر** لوحي من Dell). يتم عرض الرمز المكون من حروف وأرقام الذي يحتوي على خمسة أحرف على الجهاز المحمول.

على جهاز الكمبيوتر اللوحي Dell

1 اضغط على رمز **DDP|ST Mobile Pairing**.

يتم عرض رسالة حالة يظهر بها، *لا يوجد جهاز مقترن*.

ملاحظة: إذا تم عرض رسالة توضح أنه تم إلغاء تمكين كلمة المرور الصالحة لمرة واحدة، تحقق بالرجوع إلى المسؤول لديك إذا ما أمكن تمكينها.

2 في أسفل الشاشة، اضغط على **تسجيل جهاز**.

3 أدخل معرّف فريد للجهاز المحمول، على سبيل المثال "MySmartphone". وفي وقت لاحق، إذا نسيت كلمة المرور لجهاز الكمبيوتر اللوحي الخاص بك، يسرد جهاز الكمبيوتر اللوحي هذا الاسم لتذكيرك بالجهاز المحمول الذي يمكن استخدامه لاستعادة إمكانية الوصول إلى جهاز الكمبيوتر اللوحي من خلال كلمة المرور الصالحة لمرة واحدة.

4 في حقل رمز التعليمة البرمجية المتنقلة لجهاز الكمبيوتر اللوحي، أدخل رمز التعليمة البرمجية المتنقلة المكون من خمسة أحرف مكونة من حروف وأرقام من خلال الجهاز المحمول / الهاتف الذكي.

5 اضغط **التالي**. يتم عرض رمز الاقتران.

على الجهاز المحمول أو الهاتف الذكي

1 في أسفل الشاشة، اضغط على **إقران الأجهزة**.

2 اضغط على **الإدخال اليدوي**.

ملاحظة: لا يتوفر حالياً فحص رمز الاستجابة السريعة لأجهزة الكمبيوتر اللوحي.

3 اكتب رمز الاقتران الذي يُعرض على جهاز الكمبيوتر اللوحي من Dell. لا تحتاج إلى كتابة مسافات.

4 اضغط على **تم**.

5 اضغط على **إقران الأجهزة**.

يتم عرض رمز تحقق رقمي مكون من 6 إلى 10 أرقام.

على جهاز الكمبيوتر اللوحي Dell

1 اضغط **التالي**.

2 اضغط على حقل رمز التحقق، واكتب رمز التحقق المعروض على جهاز الهاتف المحمول / الهاتف الذكي.
يقوم هذا الرمز الرقمي المكون من 6 إلى 10 أرقام بالتحقق من اقتران الجهازين.

ملاحظة: إذا تجاوزت الحد الأقصى من عدد إعادة محاولات إدخال الرمز الصحيح، يجب عليك إعادة إجراء عملية الإقران.

3 اضغط على **إرسال**.
في حقل الحالة، يتم عرض اسم جهاز الهاتف المحمول المقترن.

على الجهاز المحمول أو الهاتف الذكي

1 اضغط **التالي**.
يطالبك مربع الحوار بالتأكد من أنك أكملت التسجيل.

2 اضغط على **المتابعة**.
تظهر علامة اختيار خضراء ورسالة لتأكيد التسجيل.

3 اضغط على رمز التعديل لإدخال اسم وصفي لجهاز الكمبيوتر اللوحي لديك.

4 اضغط على **انتهاء**.

استعادة كلمة المرور الخاصة بك

لاستعادة كلمة المرور الخاصة بجهاز الكمبيوتر اللوحي، يجب أن تقوم مسبقاً بإقران جهاز الكمبيوتر اللوحي من Dell بهاتف محمول.

على الجهاز المحمول أو الهاتف الذكي 

1 قم بتشغيل تطبيق **Dell Security Tools**، أدخل رمز PIN واضغط على **تسجيل الدخول**.
يتم عرض اسم جهاز الكمبيوتر اللوحي المقترن.

2 في أسفل الشاشة، اضغط على الرمز  المجاور لكلمة المرور الصالحة لمرة واحدة.
يتم عرض كلمة المرور الرقمية الصالحة لمرة واحدة.

على جهاز الكمبيوتر اللوحي Dell

1 في شاشة تسجيل الدخول، اضغط على **لا يمكنني الوصول إلى حسابي**.
تسرد الشاشة الاسم الذي قمت بإنشائه لجهاز الهاتف المحمول المقترن بجهاز الكمبيوتر اللوحي.

2 في حقل كلمة المرور الصالحة لمرة واحدة، اكتب كلمة المرور التي يعرضها جهاز الهاتف المحمول الخاص بك.

3 اضغط على **إلغاء القفل**.

4 قم بتحديد **نمط**، أو **رمز PIN**، أو **كلمة مرور**.

ملاحظة: إذا لم تقم بإدخال نمط جديد أو رمز PIN جديد أو كلمة مرور جديدة الآن، ستظل كلمة المرور المنسية السابقة الخاصة بك كما هي.

5 في شاشة التشفير، حدد أحد الخيارات واضغط على **متابعة**.

6 أدخل كلمة المرور الجديدة واضغط على **متابعة**.

7 قم بتأكيد كلمة المرور الجديدة واضغط على **موافق**.

8 في شاشة الإعدادات، قم بتحديد أحد تفضيلات الإخطار واضغط على **تم**.

إلغاء اقتران جهاز

على جهاز الكمبيوتر اللوحي Dell

1 على جهاز الكمبيوتر اللوحي، قم بتشغيل تطبيق **DDP|ST Agent**.

2 قم بتسجيل الدخول باستخدام عنوان خادم DDP.

3 اضغط على رمز **DDP|ST Mobile Pairing**.

4 في الجزء السفلي، اضغط على **إلغاء الاقتران**.

5 اضغط على **المتابعة** لتأكيد رغبتك في إلغاء إقران الجهاز.
يظهر في الحالة، *لا يوجد جهاز مقترن*.

على الجهاز المحمول أو الهاتف الذكي

1 في تطبيق أدوات التأمين Dell Security Tools المقدم من Dell، اضغط على شريط العنوان الخاص بأدوات التأمين Security Tools لفتح شاشة التنقل navigation drawer.

2 اضغط على **إزالة أجهزة كمبيوتر**.

3 انقر على مربع الاختيار المجاور للاسم الذي قمت بإنشائه لجهاز الكمبيوتر المحمول من Dell.

4 في الجزء السفلي، اضغط على **إزالة**.

5 في مربع الحوار الخاص بالتأكيد، اضغط على **المتابعة**.

تسجيل جهاز جديد

عندما تقوم بتسجيل جهاز جديد بنجاح، يقوم جهاز الكمبيوتر اللوحي تلقائياً بإلغاء إقرانه بجهاز الهاتف المحمول السابق.

لتسجيل جهاز جديد:

1 على جهاز الكمبيوتر اللوحي، قم بتشغيل تطبيق **DDP|ST Agent**.

2 قم بتسجيل الدخول باستخدام عنوان خادم DDP.

3 اضغط على رمز **DDP|ST Mobile Pairing**.

4 في الجزء السفلي، اضغط على **تسجيل جهاز جديد**.

5 اضغط على **المتابعة** لتأكيد رغبتك في إلغاء اقتران جهاز الهاتف المحمول الحالي وتسجيل جهاز جديد.

6 الاستمرار في تسجيل الأجهزة وإقرانها.

استخدام DDP|ST Password Manager

يسمح Password Manager لك بإنشاء كلمة مرور رئيسية واحدة للوصول إلى حساب Password Manager الخاص بك، ومنه يمكنك إدارة كلمات المرور المستخدمة في المواقع وتطبيقات الهاتف المحمول ومصادر الشبكة. يمكنك من خلال Password Manager:

- إنشاء أسماء لفئات الموقع، على سبيل المثال، *البريد الإلكتروني*، *تخزين مجموعة النظراء*، *الاتصال*، *الأخبار*، *برامج التحرير*، *التواصل الاجتماعي*.
- قم بإنشاء حسابات حيث يمكنك تخزين اسم المستخدم وبيانات اعتماد كلمة المرور للمواقع وتطبيقات البرامج ثم استخدم Password Manager لتسجيل الدخول تلقائياً.
- قم بتعديل كلمة المرور الرئيسية أو كلمات المرور الأخرى.
- قم بعمل نسخة احتياطية لبيانات اعتماد تسجيل الدخول المخزنة واستعادتها.

إنشاء كلمة مرور رئيسية وحساب جديد

1 في شاشة التطبيقات "APPS drawer" في جهاز الكمبيوتر اللوحي، اضغط على رمز **DDP|ST Agent**  .

2 في شاشة DDP|ST Agent، اضغط على رمز **DDP|ST Password Manager**.

يتم عرض شاشة Dell Password Manager.

3 اضغط على حقل **كلمة المرور** ثم قم بإدخال كلمة مرور رئيسية.

ملاحظة: قام المسؤول لديك بتعيين المتطلبات الخاصة بالطول والأحرف.

4 تأكيد كلمة المرور.

5 اضغط على **تسجيل الدخول**.

يتم عرض شاشة DDP|ST Password Manager.

ملاحظة: قبل الضغط على رمز + (الإضافة) لإنشاء حساب جديد، فإن أفضل ممارسة هي تحديد الفئات التي تريد استخدامها لحسابات موقع الويب أولاً. راجع إنشاء فئات لحسابات الموقع.

قم بتسجيل الدخول إلى DDP|ST Password Manager

1 في شاشة DDP|ST Agent، اضغط على رمز **DDP|ST Password Manager**.

2 اضغط على حقل **كلمة المرور** ثم أدخل كلمة المرور الرئيسية الخاصة بك.

3 اضغط على **تسجيل الدخول**.

إذا استمر عدم التنشيط لديك لمدة من الوقت حددها المسؤول، فسيتم إغلاق Password Manager وعرض شاشة تسجيل الدخول باستخدام كلمة المرور. كرر خطوة 2 وخطوة 3 المذكورة فيما سبق.

إنشاء فئات لحسابات الموقع

عندما تستخدم Password Manager لتخزين كلمة المرور للموقع، يسمح لك ذلك بتحديد فئة لحساب الموقع. تشتمل الفئات الموجودة على فئة المفضلات، وفئة العمل، والفئة الشخصية. قبل إنشاء حساب جديد للموقع، حدد إذا ما كنت تريد فئات إضافية.

لإنشاء فئة لحسابات الموقع:

1 في الجزء العلوي، اضغط على **كل الفئات** وحدد **فئة جديدة**.

2 اكتب اسم الفئة، على سبيل المثال، *البريد الإلكتروني*، *تخزين مجموعة النظراء*، *الاتصال*، *الأخبار*، *برامج التحرير*، *التواصل الاجتماعي*.

3 في أعلى الجانب الأيمن، اضغط على **حفظ**.

يتم عرض الفئة التالية في القائمة.

تنظيم الفئات

1 في أعلى الجانب الأيسر، اضغط على شريط العنوان لفتح شاشة التنقل "navigation drawer".

2 اضغط على **الإعدادات**.

3 اضغط على **تنظيم الفئات**.

4 اضغط مع الاستمرار على صف الفئة حتى يتم تمييز الصف. ثم اسحبه إلى موقع مختلف.

إنشاء حسابات مواقع جديدة

استخدم شاشة حساب Password Manager لإضافة حسابات.

لإنشاء حسابات مواقع جديدة:

1 في شريط العنوان، اضغط على + (رمز الإضافة).

يتم عرض شاشة حساب Password Manager.

2 في حقل الوصف، أدخل عنوان أو وصف لهذا الحساب.

3 بشكل اختياري، اضغط على رمز **النجمة** للإشارة إلى هذا الحساب كحساب مفضل.

4 وفي الجزء الأيمن، اضغط على حقل الفئة وحدد فئة.

لمزيد من المعلومات، راجع إنشاء فئات لحسابات الموقع.

5 اضغط على حقل **الموقع** وأدخل عنوان الموقع "URL".

6 اضغط على حقل **اسم المستخدم** وأدخل اسم المستخدم لهذا الموقع.

7 في الجزء الأيمن من حقل **كلمة المرور**، اضغط على رمز برنامج إنشاء كلمة المرور "Password Generator".

يقوم Password Manager تلقائياً بإنشاء كلمة المرور. لتعديل قوة كلمة المرور، راجع تحديد إعدادت برنامج إنشاء كلمة المرور "Password Generator".

ملاحظة: إذا قمت بإدخال كلمة مرور بدلاً من استخدام برنامج إنشاء كلمة المرور "Password Generator"، فسيتضح من خلال شريط التمرير إذا ما كانت كلمة المرور سيئة أو ضعيفة أو متوسطة أو جيدة أو الأفضل.

8 في أعلى الجانب الأيمن، اضغط على **حفظ**.

يتم إضافة الحساب إلى شاشة Password Manager الرئيسية.

استخدام خيارات القائمة لحسابات الموقع

بعد أن تقوم بإعداد العديد من حسابات الموقع، يمكنك استخدام الرموز في شريط العنوان للقيام بـالآتي:

- البحث عن حساب.
- تحرير حساب الموقع أو كلمة المرور، أو تحديده كحساب مفضل.
- في قائمة تجاوز السعة، يمكنك تصنيف الحساب أو حذفه.

تصنيف حسابات المواقع حسب الترتيب الأبجدي أو حسب الأولوية

1 في أعلى الجانب الأيمن من شاشة Password Manager الرئيسية، اضغط على رمز **قائمة تجاوز السعة**.

2 اضغط على **التصنيف حسب**.

3 حدد خيار الترتيب الأبجدي أو حسب الأولوية.

4 لعرض حسابات الموقع داخل فئة واحدة فقط، حدد خيار من قائمة الفئات.

تعديل الإعدادات

يمكنك تعديل طول كلمة المرور والخصائص، وكلمة المرور الرئيسية الخاصة بك، ومدة التخزين في الحافظة.

لتعديل الإعدادات:

1 في أعلى الجانب الأيسر، اضغط على شريط العنوان لفتح شاشة التنقل "navigation drawer".

2 اضغط على **الإعدادات**.

تحديد إعدادت برنامج إنشاء كلمة المرور "Password Generator"

1 في الإعدادات، اضغط على **برنامج إنشاء كلمة المرور "Password Generator"**.

2 تعديل طول كلمة المرور.

3 حدد مربع الاختيار للسماح بالأحرف الكبيرة والصغيرة والأرقام والرموز. قم بإلغاء تحديد مربع الاختيار لمنع الاستخدام.

4 في أعلى الجانب الأيمن، اضغط على **حفظ**.

تعديل مدة التخزين في الحافظة.

1 ضمن الإعدادات، اضغط على **مدة التخزين في الحافظة.**

2 قم بتعديل الإعدادات. تشتمل الخيارات على مجموعة تتراوح بين *15 ثانية* و*10 دقائق*.

3 اضغط على **تم**.

تغيير كلمة المرور الرئيسية

1 في الإعدادات، اضغط على **كلمة المرور الرئيسية**.

2 قم بإكمال كل حقل.

3 اضغط على **حفظ** في أعلى الجانب الأيمن.

قم بعمل نسخة احتياطية لمعلومات تسجيل الدخول وتخزينها في DDP|ST Password Manager

1 في أعلى الجانب الأيسر، اضغط على رمز **DDP** لفتح شاشة التنقل "navigation drawer".

2 اضغط على **إعدادات** > **قاعدة بيانات إدارة كلمة المرور**.

ملاحظة: يتم عرض تاريخ آخر نسخة احتياطية، إن أمكن.

3 عليك القيام بإحدى الخطوات التالية:

- اضغط على **النسخة الاحتياطية لحسابات إدارة كلمة المرور**، ثم **إنشاء نسخة احتياطية الآن**.
- اضغط على **استعادة حسابات إدارة كلمة المرور** ثم **الاستعادة الآن**.

تسجيل الخروج من DDP|ST Password Manager

1 في أعلى الجانب الأيسر، اضغط على شريط العنوان لفتح شاشة التنقل "navigation drawer".

2 اضغط على **تسجيل الخروج**.

التحديث التلقائي لتطبيقات DDP|ST

افتراضياً، يتم تعيين تطبيقات DDP|ST Mobile Pairing DDP|ST Password Manager على وضع *التحديث التلقائي*.

التحديث التلقائي هو أفضل ممارسة لضمان أن يتم تطبيق تحديثات التأمين فوراً.

لعرض هذه الإعدادات:

1 من شاشة التنقل "navigation drawer" في Google Play Store، اضغط على **تطبيقاتي**.

2 اضغط على رمز **قائمة تجاوز السعة**.

3 لإجراء التحديث التلقائي، تأكد من تحديد مربع الاختيار.

ملاحظة: إذا قام مستخدم واحد بتحديث التطبيق يدوياً، فسيتم تطبيق التحديث على كل حسابات المستخدم على ذلك الكمبيوتر اللوحي بناءً على الإسلوب المتبع لنظام Android

تسجيل الخروج من DDP|ST Agent

1 انتقل إلى شاشة **DDP|ST Agent**.

2 في أعلى الجانب الأيمن، اضغط على **تسجيل الخروج**.

إلغاء تثبيت DDP|ST Agent

إذا كنت تخطط لاستخدام DDP|ST لنظام Android مرة أخرى في المستقبل، تنصحك شركة Dell **بعدم** إلغاء تثبيت DDP|ST Agent.

ملاحظة: إذا قمت بإلغاء تثبيت DDP|ST Agent، فلن يتم تفعيل الوضع التجاري الخاص بـ DDP|ST لنظام Android مرةً أخرى. لن يتم عرض DDP|ST Password Manager وتطبيقات إقران الهاتف المحمول مرةً أخرى. ستظل بياناتك موجودة في حال رغبتك في إعادة التثبيت في وقت لاحق.

لإلغاء التثبيت:

1 اضغط على **إعدادات** > **التطبيقات**.

2 اضغط على علامة التبويب **تم التنزيل**.

3 اضغط على **DDP|ST Agent**.

4 اضغط على **إلغاء تثبيت**.


0XXXXXA0X