

Dell Data Protection

Guida dell'amministratore di Security Tools per Android



© 2015 Dell Inc.

Marchi registrati e marchi commerciali utilizzati nella suite di documenti DDP|E, DDP|ESS, DDP|ST e DDP|CE: Dell™ e il logo Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® e KACE™ sono marchi commerciali di Dell Inc. McAfee® e il logo McAfee sono marchi commerciali o marchi registrati di McAfee, Inc. negli Stati Uniti e in altri Paesi. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® e Xeon® sono marchi registrati di Intel Corporation negli Stati Uniti e in altri Paesi. Adobe®, Acrobat® e Flash® sono marchi registrati di Adobe Systems Incorporated. Authen Tec® ed Eikon® sono marchi registrati di Authen Tec. AMD® è un marchio registrato di Advanced Micro Devices, Inc. Microsoft®, Windows® e 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® e Visual C++® sono marchi commerciali o marchi registrati di Microsoft Corporation negli Stati Uniti e/o in altri Paesi. VMware® è un marchio registrato o marchio commerciale di VMware, Inc. negli Stati Uniti o in altri Paesi. Box® è un marchio registrato di Box. DropboxSM è un marchio di servizio di Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube® e Google™ Play sono marchi commerciali o marchi registrati di Google Inc. negli Stati Uniti e in altri Paesi. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloudSM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® e Siri® sono marchi di servizio, marchi commerciali o marchi registrati di Apple, Inc. negli Stati Uniti e/o in altri Paesi. GO ID®, RSA® e SecurID® sono marchi registrati di EMC Corporation. EnCase™ e Guidance Software® sono marchi commerciali o marchi registrati di Guidance Software. Entrust® è un marchio registrato di Entrust®, Inc. negli Stati Uniti e in altri Paesi. InstallShield® è un marchio registrato di Flexera Software negli Stati Uniti, in Cina, nella Comunità Europea, ad Hong Kong, in Giappone, in Taiwan e nel Regno Unito. Micron® e RealSSD® sono marchi registrati di Micron Technology, Inc. negli Stati Uniti e in altri Paesi. Mozilla® Firefox® è un marchio registrato di Mozilla Foundation negli Stati Uniti e/o in altri Paesi. iOS® è un marchio commerciale o marchio registrato di Cisco Systems, Inc. negli Stati Uniti e in alcuni altri Paesi, ed è concesso in licenza. Oracle® e Java® sono marchi registrati di Oracle e/o sue affiliate. Altri nomi possono essere marchi commerciali dei rispettivi proprietari. SAMSUNG™ è un marchio commerciale di SAMSUNG negli Stati Uniti o in altri Paesi. Seagate® è un marchio registrato di Seagate Technology LLC negli Stati Uniti e/o in altri Paesi. Travelstar® è un marchio registrato di HGST, Inc. negli Stati Uniti e in altri Paesi. UNIX® è un marchio registrato di The Open Group. VALIDITY™ è un marchio commerciale di Validity Sensors, Inc. negli Stati Uniti e in altri Paesi. VeriSign® e altri marchi correlati sono marchi commerciali o marchi registrati di VeriSign, Inc. o sue affiliate o filiali negli Stati Uniti e in altri Paesi, e sono concessi in licenza a Symantec Corporation. KVM on IP® è un marchio registrato di Video Products. Yahoo!® è un marchio registrato di Yahoo! Inc.

In questo prodotto vengono utilizzate parti del programma 7-Zip. Il codice sorgente è disponibile all'indirizzo www.7-zip.org. La gestione delle licenze è basata sulla licenza GNU LGPL + restrizioni unRAR (www.7-zip.org/license.txt).

2015-10

Protetto da uno o più brevetti statunitensi, tra cui: numero 7665125; numero 7437752; e numero 7665118.

Le informazioni contenute nel presente documento sono soggette a modifica senza preavviso.

Sommario

1	Panoramica di Security Tools per Android	5
	Requisiti	5
2	Attività dell'amministratore	7
	Abilitare la protezione in DDP Server	7
	Impostare gli account utente nel DDP Server	7
	Inviare notifiche agli utenti	7
	Abilitare il recupero della Password monouso (OTP)	8
	Configurare DDP ST Password Manager	8
	Abilitare DDP ST Password Manager	8
	Impostare i requisiti per i passcode principali di Password Manager	9
	Specificare il periodo di tempo per l'inattività	9
	Risoluzione dei problemi	9
3	Esperienza dell'utente finale	11
	Impostare un'opzione di blocco schermo nel tablet	11
	Scaricare ed eseguire l'app DDP ST Agent	11
	Registrare e associare i dispositivi	11
	Recuperare la password	13
	Annullare l'associazione di un dispositivo	13
	Nel tablet Dell	13
	Nel dispositivo mobile o smartphone	13
	Registrare un nuovo dispositivo	14
	Usare DDP ST Password Manager	14
	Creare una password principale e un nuovo account	14
	Accedere a DDP ST Password Manager	14
	Creare categorie per account di siti Web	15
	Creare nuovi account di siti Web	15
	Usare le opzioni di menu degli account di siti Web	15
	Modificare le impostazioni	16

Eseguire il backup e ripristinare le informazioni di accesso in DDP ST Password Manager	16
Disconnettersi da DDP ST Password Manager.	16
Aggiornare automaticamente le app DDP ST	17
Disconnettersi da DDP ST Agent.	17
Disinstallare DDP ST Agent	17

Panoramica di Security Tools per Android

Dell Data Protection | Security Tools (DDP|ST) for Android è una soluzione per la sicurezza degli endpoint per uso aziendale nei tablet Dell supportati.

Inizialmente, un tablet Dell è in modalità commerciale. Per abilitare e usare le funzioni di DDP|ST for Android, è necessario passare il tablet in modalità commerciale. Per maggiori informazioni, consultare [Scaricare ed eseguire l'app DDP|ST Agent](#).

Requisiti

Tablet

Questa tabella elenca i tablet supportati.

Tablet
<ul style="list-style-type: none">Dell Venue 8 7840
<ul style="list-style-type: none">Dell Venue 10 7040

Sistemi operativi mobili

Security Tools per Android

Questa tabella elenca i sistemi operativi supportati dai tablet Dell.

Sistemi operativi Android
<ul style="list-style-type: none">5.0 - 5.1 Lollipop

Dell Security Tools Mobile

Questa tabella elenca i sistemi operativi supportati da Security Tools quando si associa un altro dispositivo mobile ai tablet Dell.

Sistemi operativi Android
<ul style="list-style-type: none">4.0 - 4.0.4 Ice Cream Sandwich4.1 - 4.3.1 Jelly Bean4.4 - 4.4.4 KitKat
<ul style="list-style-type: none">5.0 - 5.1 Lollipop
Sistemi operativi iOS
<ul style="list-style-type: none">iOS 7.xiOS 8.x
Sistemi operativi Windows
<ul style="list-style-type: none">Windows 8.1 PhoneWindows 10 Mobile

Criteri

Per informazioni dettagliate sui criteri di DDP|ST for Android consultare la *Guida dell'amministratore*, disponibile nella console di gestione remota. Vengono anche visualizzate le descrizioni dei criteri come suggerimenti nella Remote Management Console.

È possibile abilitare i criteri di DDP|ST for Android ai livelli seguenti:

- Aziendale
- Dominio
- Gruppi di utenti
- Utenti

Attività dell'amministratore

Abilitare la protezione in DDP Server

Per abilitare la protezione nel Dell Enterprise Server o nel DDP Enterprise Server - VE (Virtual Edition) per tablet che in cui è in esecuzione DDP|ST, aprire la Remote Management Console ed assicurarsi che il criterio *Protezione abilitata* di Android sia impostato su **Vero** (predefinito). Questo è il criterio principale per tutti gli altri criteri di DDP|ST for Android:

- *Vero* – Il DDP Server gestisce le app di DDP nel tablet Dell.
- *Falso* – Il DDP Server non gestisce le app di DDP nel tablet Dell. Pertanto, altre impostazioni dei criteri di DDP|ST for Android sono irrilevanti.

Impostare gli account utente nel DDP Server

Per impostare gli account utente nel DDP Server:

- 1 Eseguire l'accesso alla Remote Management Console come amministratore Dell.
- 2 Nel riquadro sinistro, fare clic su **Protezione e gestione > Domini**.
- 3 Fare clic sull'icona **Membri** del dominio a cui si desidera aggiungere un utente.
- 4 Fare clic su **Aggiungi utenti**.
- 5 Immettere un filtro per cercare il nome utente per *Nome comune*, *Nome principale utente (UPN, Universal Principal Name)* o *sAMAccountName*. Il carattere jolly è `*`.

È necessario definire Nome comune, Nome principale utente e sAMAccountName per ogni utente nel server di directory aziendale. Se un utente è membro di un gruppo o di un dominio, ma non viene visualizzato nell'elenco dei membri del gruppo o del dominio nella Remote Management Console, assicurarsi che tutti e tre i nomi siano stati definiti correttamente per l'utente nel server di directory aziendale.

La query eseguirà automaticamente la ricerca per Nome comune, UPN e infine sAMAccountName, finché non viene trovata una corrispondenza.

- 6 Selezionare gli utenti da aggiungere al dominio dall'Elenco utenti directory. Utilizzare **<MAIUSC> <clic>** o **<Ctrl> <clic>** per selezionare più utenti.
- 7 Fare clic su **Aggiungi selezionati**.

Inviare notifiche agli utenti

Quando gli account utente sono configurati, gli utenti devono scaricare l'app DDP|ST Agent e quindi attivarla nel DDP Server.

- Inviare notifiche agli utenti quando gli account sono configurati.
- Indicare agli utenti se scaricare l'app DDP|ST Agent da Google Play Store o da un altro percorso.
- Comunicare loro quali credenziali usare per l'accesso.
- Inviare loro l'indirizzo del DDP Server da usare per l'accesso.
- Se si abilita DDP|ST Password Manager, informare gli utenti dei requisiti di lunghezza e tipo di caratteri per la password principale.

Abilitare il recupero della Password monouso (OTP)

Questa funzionalità consente agli utenti che dimenticano la password di ricevere una password monouso per sbloccare il tablet Dell e reimpostare la password. Per abilitare questa funzionalità, è prima necessario associare il tablet ad uno smartphone o dispositivo mobile in cui l'app Dell Security Tools è in esecuzione.

Il criterio *Ripristino OTP abilitato* è il criterio principale per tutti gli altri criteri della Password monouso. La schermata di accesso verifica il criterio prima di consentire il ripristino della Password monouso, anche se il tablet è associato.

Per abilitare il ripristino della Password monouso:

- 1 Nella Remote Management Console, impostare il criterio *Ripristino OTP abilitato* su **Vero**.
 - *Vero* – La funzione di Ripristino password monouso è abilitata e consente all'utente di utilizzare un dispositivo mobile associato per generare password monouso per sbloccare l'account, nel caso in cui abbia smarrito la password dell'account.
 - *Falso* (predefinito) – L'utente non potrà utilizzare il ripristino password monouso per sbloccare l'account, a prescindere dagli altri valori del criterio password monouso.
- N.B.** Quando un utente apre l'app DDP|ST Mobile Pairing per associare dei dispositivi, l'app verifica prima che il Ripristino password monouso sia stato abilitato. Se il criterio Ripristino OTP abilitato è impostato su Falso o viene modificato su Falso dopo che l'utente ha associato il proprio tablet ad altri dispositivi, l'icona di DDP|ST Mobile Pairing non è visibile nel tablet dell'utente.
- 2 Impostare il valore per *N. max tentativi di ripristino OTP*. Le opzioni sono 5-10 con un valore predefinito di 5.
- 3 Impostare il valore per *Azione per errore n. max tentativi di ripristino OTP*.
- 4 L'opzione predefinita è *Annulla associazione*, in questo caso l'associazione tra il tablet e il dispositivo mobile viene annullata e il Ripristino password monouso disabilitato.
- 5 Eseguire il commit dei criteri.

Configurare DDP|ST Password Manager

L'app DDP|ST Password Manager consente all'utente di gestire le password in modo protetto. L'utente può archiviare tutte le password all'interno dell'app, la quale protegge le password con una chiave principale. La chiave principale può essere sbloccata solo con la password principale. L'utente deve ricordarsi solo la password principale per accedere a tutte le altre password archiviate in DDP|ST Password Manager.

Abilitare DDP|ST Password Manager

Per abilitare Password Manager nella Remote Management Console, impostare il criterio *Abilita Password Manager* su **Vero**. Questo è il criterio principale per Password Manager.

- *Vero* - Password Manager è disponibile, accetta e archivia le nuove credenziali di accesso dell'utente.
- *Falso* (predefinito) - Password Manager non è disponibile, a prescindere dagli altri valori del criterio.

Impostare i requisiti per i passcode principali di Password Manager

È possibile impostare i requisiti per i passcode principali di Password Manager impostando i seguenti criteri:

- 1 Specificare il valore *Lunghezza minima passcode*:
 - 0-18 caratteri (il valore predefinito è 8)
- 2 Specificare i valori del criterio per i caratteri:
 - *Consenti caratteri semplici nel passcode*
 - *Vero* (predefinito) – Il passcode può contenere caratteri ripetuti o crescenti/decrescenti (come ABC o 321).
 - *Falso* – I passcode semplici non sono consentiti.
 - *Richiedi caratteri alfanumerici nel passcode*
 - *Vero* (predefinito) – Il passcode deve contenere una combinazione di lettere e numeri.
 - *Falso* – Nel passcode non sono necessari caratteri alfanumerici.
 - *Numero minimo di caratteri complessi nel passcode*
 - 0-4 caratteri (il valore predefinito è 1)
 - I caratteri complessi sono caratteri diversi da numeri e lettere (&%\$#)
- 3 Assicurarsi di inviare una notifica agli utenti finali riguardo ai requisiti impostati per il passcode principale.

Specificare il periodo di tempo per l'inattività

È possibile specificare il numero di minuti per cui un dispositivo può rimanere inattivo (senza input dell'utente) prima che Password Manager venga bloccato. Al raggiungimento di tale limite, Password Manager viene bloccato e l'utente deve immettere il passcode. Impostare da 1 a 60 minuti nel criterio *Periodo di inattività per blocco app Password Manager*. L'impostazione predefinita è 5 minuti.

Risoluzione dei problemi

Non posso effettuare l'accesso con l'indirizzo del DDP Server o non posso accedere alle app DDP|ST Agent.

Consultare [Impostare un'opzione di blocco schermo nel tablet](#).

Viene visualizzato il messaggio di errore: La funzionalità multiutente di Android commerciale non è supportata.

Attualmente, solo l'account del proprietario di un tablet è supportato con Android commerciale.

Il mio tablet non è più associato al dispositivo originale.

È stato registrato un nuovo dispositivo? In questo modo si annulla automaticamente l'associazione del dispositivo precedente.

Le app DDP|ST Password Manager e DDP|ST Mobile Pairing non vengono più visualizzate.

È stato toccato **Disinstalla** nell'app DDP|ST Agent? In questo caso le altre due app sono disabilitate e non vengono più visualizzate, tuttavia i dati esistono ancora. Se si esegue l'app DDP|ST Agent e la si attiva con il DDP Server, le altre app verranno visualizzate e i dati saranno disponibili.

Ho toccato l'icona di DDP|ST Password Manager, ma non ho visualizzato niente.

Verificare con l'amministratore se la password monouso è abilitata e chiedere se è un'opzione disponibile.

Esperienza dell'utente finale

Per usare DDP|ST for Android, è necessario convertire il proprio tablet Dell dalla modalità consumatore alla modalità commerciale. L'amministratore:


- Invierà notifica dell'avvenuta configurazione dell'account utente di DDP|ST for Android
- Indicherà le credenziali di accesso
- Invierà l'indirizzo di accesso a DDP Server
- Indicherà i requisiti di lunghezza e tipo di caratteri per la password principale di Password Manager

Impostare un'opzione di blocco schermo nel tablet

Per la protezione avanzata durante l'utilizzo di DDP|ST for Android, è necessario impostare un blocco schermo. Prima di usare l'app DDP|ST Agent, andare a **Impostazioni > Sicurezza > Blocco schermo** nel tablet Dell e impostare una combinazione, un PIN o una password, altrimenti non sarà possibile accedere alle app DDP|ST Agent.

Scaricare ed eseguire l'app DDP|ST Agent

Per iniziare:

- 1 Scaricare l'app DDP|ST Agent nel tablet .
N.B. La propria azienda indicherà se effettuare il download dell'app da Google Play Store o da un altro percorso.
- 2 Nell'APP drawer del tablet, toccare l'icona DDP|ST Agent.
Viene visualizzata la schermata Dell Data Protection | ST Agent.
- 3 Toccare **Accetto** per il contratto di licenza.
- 4 Immettere l'indirizzo di DDP Server.
- 5 Immettere nome di accesso e password in base alle informazioni ricevute dall'amministratore.
- 6 Toccare **Accedi**.

Il tablet è ora in modalità commerciale e DDP|ST Agent visualizza queste app:

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

Registrare e associare i dispositivi

Associare il tablet Dell ad un altro dispositivo mobile consente il recupero della password nel caso in cui l'utente la dimentichi.

- Nel tablet Dell, [Scaricare ed eseguire l'app DDP|ST Agent](#).
- Nell'altro dispositivo mobile o smartphone, installare e aprire l'app **Dell Security Tools Mobile** .

N.B. La propria azienda indicherà se effettuare il download dell'app da Google Play Store o da un altro percorso.

Nel dispositivo mobile o smartphone

- 1 Eseguire una delle azioni seguenti:
 - Se l'app **Dell Security Tools** è stata già installata, toccare **Ignora**, quindi la **guida introduttiva**, infine creare e confermare un PIN.
 - Se è già stata installata, eseguire l'app **Dell Security Tools**, immettere il PIN e toccare **Accedi**.

- 2 Nella parte inferiore della schermata successiva, toccare **Registra un computer** (questa fase si applica anche durante la registrazione di un tablet Dell).

Nel dispositivo mobile viene visualizzato un codice alfanumerico mobile contenente cinque caratteri.

Nel tablet Dell

- 1 Toccare l'icona **DDP|ST Mobile Pairing**.

Viene visualizzato il messaggio di stato *Nessun dispositivo associato*.

N.B. Se viene visualizzato il messaggio che indica che la Password monouso è disabilitata, contattare l'amministratore per abilitarla.

- 2 Nella parte inferiore della schermata, toccare **Registra dispositivo**.
- 3 Immettere un identificatore univoco per il dispositivo mobile, per esempio MySmartphone. Successivamente, se l'utente ha dimenticato la password, il tablet stesso elenca il nome per ricordare quale dispositivo mobile usare per recuperare l'accesso tramite una password monouso.
- 4 Nel campo Codice mobile del tablet, immettere il codice alfanumerico mobile contenente cinque caratteri indicato nel dispositivo mobile/smartphone.
- 5 Toccare **Avanti**. Viene visualizzato un codice di associazione.

Nel dispositivo mobile o smartphone

- 1 Nella parte inferiore, toccare **Associa dispositivi**.
- 2 Toccare **Inserimento manuale**.

N.B. Attualmente la funzione Esegui scansione codice QR non è disponibile per il tablet.

- 3 Digitare il codice di associazione che viene visualizzato nel tablet Dell. Non è necessario digitare gli spazi.
- 4 Toccare **Fine**.
- 5 Toccare **Associa dispositivi**.

Viene visualizzato un codice numerico di verifica contenente da 6 a 10 cifre.

Nel tablet Dell

- 1 Toccare **Avanti**.
- 2 Toccare il campo Codice di verifica e inserire il codice di verifica visualizzato nel dispositivo mobile/smartphone.
Questo codice numerico di 6-10 cifre verifica l'associazione dei due dispositivi.

N.B. Se si supera il numero massimo di tentativi per immettere il codice corretto, è necessario riavviare il processo di associazione.

- 3 Toccare **Invia**.

Nel campo Stato viene visualizzato il nome del dispositivo mobile associato.


Nel dispositivo mobile o smartphone

- 1 Toccare **Avanti**.
Una finestra di dialogo chiede di verificare di aver completato la registrazione.
- 2 Toccare **Continua**.
Un segno di spunta verde e un messaggio confermano la registrazione.
- 3 Toccare l'icona Modifica per inserire un nome descrittivo per il tablet.
- 4 Toccare **Fine**.

Recuperare la password

Per recuperare la password del tablet, è necessario aver precedentemente associato il tablet Dell e il dispositivo mobile.

Nel dispositivo mobile o smartphone

- 1 Eseguire l'app Dell Security Tools, inserire il PIN e toccare **Accedi**.
Viene visualizzato il nome del tablet associato.
- 2 Nella parte inferiore della schermata, toccare l'icona  accanto alla Password monouso.
Viene visualizzata una Password monouso numerica.

Nel tablet Dell

- 1 Nella schermata di accesso, toccare **Non riesco ad accedere all'account**.
La schermata elenca il nome creato per il dispositivo mobile associato al tablet.
- 2 Nel campo Password monouso, digitare la password visualizzata dal dispositivo mobile.
- 3 Toccare **Sblocca**.
- 4 Selezionare **Combinazione, PIN o Password**.
N.B. Se non si inserisce una nuova combinazione, PIN o password, rimane la password precedente dimenticata.
- 5 Nella schermata Crittografia, selezionare un'opzione e toccare **Continua**.
- 6 Immettere la nuova password e toccare **Continua**.
- 7 Confermare la nuova password e toccare **OK**.
- 8 Nella schermata Impostazioni, selezionare la preferenza di notifica e toccare **Fine**.

Annullare l'associazione di un dispositivo

Nel tablet Dell

- 1 Nel tablet, eseguire l'app DDP|ST Agent.
- 2 Accedere con l'indirizzo del DDP Server.
- 3 Toccare l'icona **DDP|ST Mobile Pairing**.
- 4 Nella parte inferiore, toccare **Annulla associazione**.
- 5 Toccare **Continua** per confermare di voler annullare l'associazione del dispositivo.
Viene visualizzato lo stato *Nessun dispositivo associato*.

Nel dispositivo mobile o smartphone

- 1 Nell'app Dell Security Tools, toccare la barra del titolo Security Tools per aprire il drawer di navigazione.
- 2 Toccare **Rimuovi computer**.
- 3 Toccare la casella di controllo accanto al nome creato per il tablet Dell.
- 4 Nella parte inferiore, toccare **Rimuovi**.
- 5 Nella finestra di dialogo di conferma, toccare **Continua**.

Registrare un nuovo dispositivo

Quando si registra un nuovo dispositivo, viene automaticamente annullata l'associazione del tablet con il dispositivo mobile precedente.

Per registrare un nuovo dispositivo:


- 1 Nel tablet, eseguire l'app DDP|ST Agent.
- 2 Accedere con l'indirizzo del DDP Server.
- 3 Toccare l'icona DDP|ST Mobile Pairing.
- 4 Nella parte inferiore, toccare **Registra nuovo dispositivo**.
- 5 Toccare **Continua** per confermare di voler annullare l'associazione del dispositivo mobile corrente e registrarne uno nuovo.
- 6 Continuare con [Registrare e associare i dispositivi](#).

Usare DDP|ST Password Manager

Password Manager consente di creare una singola password principale per accedere all'account Password Manager da cui è quindi possibile gestire le password usate in siti Web, applicazioni mobili e risorse di rete. Con Password Manager è possibile:

- Creare nomi per le categorie di siti Web, come *E-mail*, *Archiviazione cloud*, *Connettività*, *News*, *Editor*, *Social Media*.
- Creare account in cui archiviare le credenziali come nome utente e password di siti Web o applicazioni software, quindi usare Password Manager per accedere automaticamente.
- Modificare la password principale o altre password.
- Eseguire il backup e ripristinare le credenziali di accesso archiviate.

Creare una password principale e un nuovo account

- 1 Nell'APP drawer del tablet, toccare l'icona DDP|ST Agent .
- 2 Nella schermata DDP|ST Agent, toccare l'icona DDP|ST Password Manager.
Viene visualizzata la schermata Dell Password Manager.
- 3 Toccare il campo **Password**, quindi inserire la password principale.
N.B. L'amministratore ha impostato requisiti di lunghezza e limite caratteri.
- 4 Confermare la password.
- 5 Toccare **Accedi**.
Viene visualizzata la schermata DDP|ST Password Manager.

N.B. Prima di premere + (più) per creare un nuovo account, la procedura consigliata è quella di determinare prima le categorie che si desidera usare per gli account di siti Web. Consultare [Creare categorie per account di siti Web](#).

Accedere a DDP|ST Password Manager

- 1 Nella schermata DDP|ST Agent, toccare l'icona DDP|ST Password Manager.
- 2 Toccare il campo **Password**, quindi immettere la password principale.
- 3 Toccare **Accedi**.

Se l'utente rimane inattivo per il periodo di tempo impostato dall'amministratore, Password Manager si chiude e viene visualizzata la schermata di accesso con password. Ripetere il [punto 2](#) e il [punto 3](#) precedenti.

Creare categorie per account di siti Web

Quando si usa Password Manager per archiviare una password per un sito Web, consente di selezionare una categoria per tale account di sito Web. Le categorie esistenti includono Preferiti, Business e Personale. Prima di creare un nuovo account di sito Web, determinare se si desiderano altre categorie.

Per creare una categoria di account di siti Web:

- 1 Nella parte superiore, toccare **Tutte le categorie** e selezionare **Nuova categoria**.
- 2 Digitare il nome di una categoria, per esempio, *E-mail*, *Archiviazione cloud*, *Connettività*, *News*, *Editor*, *Social Media*.
- 3 Nella parte superiore destra, toccare **Salva**.
La nuova categoria viene visualizzata nel menu.

Organizzare le categorie

- 1 Nella parte superiore sinistra, toccare la barra del titolo per aprire il drawer di navigazione.
- 2 Toccare **Impostazioni**.
- 3 Toccare **Organizza categorie**.
- 4 Tenere premuta la riga di una categoria finché viene evidenziata, quindi trascinarla in una posizione diversa.

Creare nuovi account di siti Web

Usare la schermata Account di Password Manager per aggiungere gli account.

Per creare nuovi account di siti Web:

- 1 Nella barra del titolo, toccare + (icona più).
Viene visualizzata la schermata Account di Password Manager.
 - 2 Nel campo Descrizione inserire un titolo o una descrizione di tale account.
 - 3 Facoltativamente, toccare l'icona a forma di stella per indicare l'account come preferito.
 - 4 A destra, toccare il campo della categoria e selezionarne una.
Per maggiori informazioni, consultare [Creare categorie per account di siti Web](#).
 - 5 Toccare il campo **Sito Web** e inserire l'URL del sito Web.
 - 6 Toccare il campo **Nome utente** e inserire il nome utente di tale sito Web.
 - 7 A destra del campo **Password**, toccare l'icona Generatore password.
Password Manager genera automaticamente una password. Per modificare il livello di crittografia della password, consultare [Selezionare le impostazioni di Generatore password](#).
- N.B.** Se si inserisce una password senza usare il Generatore password, una barra di scorrimento indica se il livello di complessità della password è **Insufficiente**, **Scarso**, **Sufficiente**, **Buono** o **Ottimo**.
- 8 Nella parte superiore destra, toccare **Salva**.
L'account viene aggiunto alla schermata principale di Password Manager.

Usare le opzioni di menu degli account di siti Web

Se si dispone di numerosi account di siti Web, è possibile usare le icone nella barra del titolo per:

- Cercare un account.
- Modificare l'account o la password di un sito Web, o identificarlo come preferito.
- Nel menu sulla barra di navigazione è possibile ordinare o eliminare un account.

Ordinare gli account di siti Web in ordine alfabetico o per priorità

- 1 Nella parte superiore destra della schermata iniziale di Password Manager, toccare l'icona del **menu sulla barra di navigazione**.
- 2 Toccare **Ordina per**.
- 3 Selezionare l'opzione ordine alfabetico o priorità.
- 4 Per visualizzare gli account di siti Web in una sola categoria, selezionare un'opzione dal menu **Categorie**.

Modificare le impostazioni

È possibile modificare lunghezza e caratteristiche della password, la password principale e il timeout degli Appunti.

Per modificare le impostazioni:

- 1 Nella parte superiore sinistra, toccare la barra del titolo per aprire il drawer di navigazione.
- 2 Toccare **Impostazioni**.

Selezionare le impostazioni di Generatore password

- 1 In Impostazioni, toccare **Generatore password**.
- 2 Modificare la lunghezza della password.
- 3 Selezionare la casella di controllo per consentire maiuscole, minuscole, numeri e simboli. Deselezionare la casella di controllo per impedirne l'uso.
- 4 Nella parte superiore destra, toccare **Salva**.

Modificare il timeout degli Appunti

- 1 In Impostazioni, toccare **Timeout appunti**.
- 2 Modificare le impostazioni. Le opzioni variano da *15 secondi* a *10 minuti*.
- 3 Toccare **Fine**.

Modificare la password principale

- 1 In Impostazioni, toccare **Password principale**.
- 2 Completare ciascun campo.
- 3 Toccare **Salva** nell'angolo superiore destro.

Eseguire il backup e ripristinare le informazioni di accesso in DDP|ST Password Manager

- 1 Nella parte superiore sinistra, toccare l'icona **DDP** per aprire il drawer di navigazione.
- 2 Toccare **Impostazioni > Database Password Manager**.
N.B. Viene visualizzata la data dell'ultimo backup, se applicabile.
- 3 Eseguire una delle azioni seguenti:
 - Toccare **Esegui backup account Password Manager** quindi **Esegui backup ora**.
 - Toccare **Ripristina account Password Manager** quindi **Ripristina ora**.

Disconnettersi da DDP|ST Password Manager

- 1 Nella parte superiore sinistra, toccare la barra del titolo per aprire il drawer di navigazione.
- 2 Toccare **Disconnetti**.

Aggiornare automaticamente le app DDP|ST

Per impostazione predefinita, le app DDP|ST Password Manager e DDP|ST Mobile Pairing sono impostate su *Aggiorna automaticamente*.

L'aggiornamento automatico è la procedura consigliata per garantire che gli aggiornamenti della sicurezza vengano applicati immediatamente.

Per visualizzare questa impostazione:

- 1 Dal drawer di navigazione in Google Play Store, toccare **App**.
- 2 Toccare l'icona del **menu sulla barra di navigazione**.
- 3 Per l'aggiornamento automatico, accertarsi di aver selezionato la casella di controllo.

N.B. Se l'utente aggiorna automaticamente l'app, tale l'aggiornamento si applica a tutti gli account utente nel tablet in base al comportamento di Android.

Disconnettersi da DDP|ST Agent

- 1 Andare nella schermata DDP|ST Agent.
- 2 Nella parte superiore destra, toccare **Disconnetti**.

Disinstallare DDP|ST Agent

Se si prevede di usare DDP|ST for Android nuovamente in futuro, Dell consiglia di **non** disinstallare DDP|ST Agent.

N.B. Se si disinstalla DDP|ST Agent, DDP|ST for Android non sarà più in modalità commerciale. Le app DDP|ST Password Manager e Mobile Pairing non verranno più visualizzate. I dati dell'utente rimarranno per l'eventuale reinstallazione.

Per disinstallare:

- 1 Toccare **Impostazioni > App**.
- 2 Toccare la scheda **Scaricate**.
- 3 Toccare **DDP|ST Agent**.
- 4 Toccare **Disinstalla**.



0XXXXXA0X