Dell Data Protection

Security Tools for Android

Administrator Guide

© 2015 Dell Inc.

Registered trademarks and trademarks used in the DDP|E, DDP|ESS, DDP|ST, and DDP|CE suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. McAfee® and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. in the US and other countries. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, and Xeon® are registered trademarks of Intel Corporation in the U.S. and other countries. Adobe®, Acrobat®, and Flash® are registered trademarks of Adobe Systems Incorporated. Authen Tec® and Eikon® are registered trademarks of Authen Tec. AMD® is a registered trademark of Advanced Micro Devices, Inc. Microsoft®, Windows®, and 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®, and Visual C++® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® is a registered trademark or trademark of VMware, Inc. in the United States or other countries. Box® is a registered trademark of Box. Dropbox℠ is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube®, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, Aperture®, App Store℠, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®℠, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari®, and Siri® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. GO ID®, RSA®, and SecurID® are registered trademarks of EMC Corporation. EnCase™ and Guidance Software® are either trademarks or registered trademarks of Guidance Software. Entrust® is a registered trademark of Entrust®, Inc. in the United States and other countries. InstallShield® is a registered trademark of Flexera Software in the United States, China, European Community, Hong Kong, Japan, Taiwan, and United Kingdom. Micron® and RealSSD® are registered trademarks of Micron Technology, Inc. in the United States and other countries. Mozilla® Firefox® is a registered trademark of Mozilla Foundation in the United States and/or other countries. iOS® is a trademark or registered trademark of Cisco Systems, Inc. in the United States and certain other countries and is used under license. Oracle® and Java® are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. SAMSUNG™ is a trademark of SAMSUNG in the United States or other countries. Seagate® is a registered trademark of Seagate Technology LLC in the United States and/or other countries. Travelstar® is a registered trademark of HGST, Inc. in the United States and other countries. UNIX® is a registered trademark of The Open Group. VALIDITY™ is a trademark of Validity Sensors, Inc. in the United States and other countries. VeriSign® and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. KVM on IP® is a registered trademark of Video Products. Yahoo!® is a registered trademark of Yahoo! Inc.

This product uses parts of the 7-Zip program. The source code can be found at www.7-zip.org. Licensing is under the GNU LGPL license + unRAR restrictions (www.7-zip.org/license.txt).

2015-10

Protected by one or more U.S. Patents, including: Number 7665125; Number 7437752; and Number 7665118.

Information in this document is subject to change without notice.

Contents

Security Tools for Android Overview

Dell Data Protection | Security Tools (DDP|ST) for Android is an endpoint security solution for corporate use on supported Dell tablets.

Initially, a Dell tablet is in consumer mode. To enable and use the DDP|ST for Android features, you must switch the tablet to commercial mode. For more information, see Download and run the DDP|ST Agent app.

Requirements

Tablets

This table lists supported tablets.

Tablets
• Dell Venue 8 7840
• Dell Venue 10 7040

Mobile Operating Systems

Security Tools for Android

This table lists supported operating systems for the Dell tablets.

Android Operating Systems
• 5.0 - 5.1 Lollipop

Dell Security Tools Mobile

This table lists supported operating systems for Security Tools when pairing another mobile device with the Dell tablets.

Android Operating Systems
• 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
iOS Operating Systems
• iOS 7.x
• iOS 8.x
Windows Operating Systems
• Windows 8.1 Phone
• Windows 10 Mobile

Policies

For detailed information on DDP|ST for Android policies, see *Admin Help*, which is available on the Remote Management Console. Policy descriptions also display as tooltips in the Remote Management Console.

You can enable the DDP|ST for Android policies at the following levels:

- Enterprise
- Domain
- User Groups
- Users

Administrator Tasks

Enable protection on the DDP Server

To enable protection on the Dell Enterprise Server or DDP Enterprise Server - VE (Virtual Edition) for tablets running DDP|ST, open the Remote Management Console and ensure that the Androids *Protection Enabled* policy is set to **True** (default). This is the master policy for all other DDP|ST for Android policies:

- *True* – The DDP Server is managing DDP apps on the Dell tablet.
- *False* – The DDP Server is not managing DDP apps on the Dell tablet. Therefore, other DDP|ST for Android policy settings are irrelevant.

Set up user accounts on the DDP Server

To set up user accounts on the DDP Server:

1. As a Dell Administrator, log in to the Remote Management Console.
2. In the left pane, click **Protect & Manage > Domains.**
3. Click the **Members** icon of the Domain you want to add a user to.
4. Click **Add Users**.
5. Enter a filter to search the User Name by *Common Name*, *Universal Principal Name*, or *sAMAccountName*. The wild card character is *.

   A Common Name, Universal Principal Name, and sAMAccountName must be defined in the enterprise directory server for every user. If a user is a member of a Domain or Group but does not appear in the Domain or Group Members list in the Remote Management Console, ensure that all three names are properly defined for the user in the enterprise directory server.

   The query will automatically search by common name, then UPN, and then sAMAccount name until a match is found.
6. Select users from the Directory User List to add to the Domain. Use **<Shift><click>** or **<Ctrl><click>** to select multiple users.
7. Click **Add Selected**.

Notify users

After user accounts are set up, users must download the DDP|ST Agent app and then activate the app against the DDP Server.

- Notify users when their accounts are set up.
- Inform users if they should download the DDP|ST Agent app from the Google Play Store or from another location.
- Tell them which credentials to use for login.
- Send them the DDP Server address to use for login.
- If you enable DDP|ST Password Manager, inform users of the master password length and character requirements.

Enable One-Time Password (OTP) recovery

This feature allows a user who forgets their password to receive a One-time Password to unlock the Dell tablet and reset the password. To enable this feature, the tablet must first be paired with a smartphone or mobile device running the Dell Security Tools app.

The *OTP Recovery Enabled* policy is the master policy for all other One-time Password policies. The login screen checks the policy before allowing OTP recovery, even if the tablet is paired.

To enable One-time Password recovery:

1. In the Remote Management Console, set the *OTP Recovery Enabled* policy to **True**.
   - *True* – The One-time Password Recovery feature is enabled and allows the user to use a paired mobile device to generate passwords for one-time use to unlock their account if the account password is lost.
   - *False* (default) – Users will not be able to use OTP Recovery to unlock the account, regardless of other OTP policy values.

   NOTE: When a user opens the DDP|ST Mobile Pairing app to pair devices, the app first checks whether OTP Recovery has been enabled. If the OTP Recovery Enabled policy is set to False or changed to False after users have paired their tablets with other devices, the DDP|ST Mobile Pairing icon is not visible on users' tablets.
2. Set the value for *Max OTP Recovery attempts*. Options are *5-10* with a default of *5*.
3. Set the value for *Max Recover Attempts Failure Action*.
4. The default option is *Unpair*, meaning the tablet and mobile device are unpaired and One-time Password Recovery is disabled.
5. Commit the policies.

Configure DDP|ST Password Manager

The DDP|ST Password Manager app allows users to securely manage passwords. Users can store all of their passwords within the app, which protects the passwords with a master key. The master key can be unlocked only with the master password. Users must remember only their master password to access all other passwords stored in DDP|ST Password Manager.

Enable DDP|ST Password Manager

To enable Password Manager in the Remote Management Console, set the *Enable Password Manager* policy to **True**. This is the master policy for Password Manager.

- *True* - Password Manager is available and accepts and stores the user's new logon credentials.
- *False* (default) - Password Manager is not available, regardless of other policy values.

Set requirements for Password Manager master passcodes

You can set requirements for Password Manager master passcodes by setting the following policies:

1. Specify the *Minimum Passcode Length* value:
   - *0-18* characters (default is *8*)
2. Specify character policy values:
   - *Allow Simple Characters in Passcode*
     - *True* (default) – The passcode may contain repeated characters or increasing/decreasing characters (such as ABC or 321).
     - *False* – Simple passcodes are not allowed.
   - *Require Alphanumeric Characters in Passcode*
     - *True* (default) – The passcode must include a combination of letters and numbers.
     - *False* – No alphanumeric characters are required in the passcode.
   - *Minimum Complex Characters in Passcode*
     - *0-4* characters (default is *1*)
     - Complex characters are characters other than numbers or letter (&%$#)
3. Be sure to notify end users of the master passcode requirements that you set.

Specify the length of time for inactivity

You can specify the number of minutes for which a device can be idle (without user input) before Password Manager is locked. After this limit is reached, Password Manager is locked and the user must enter their passcode. Set to 1 to 60 minutes in the *Inactivity Period for Password Manager App Lock* policy. The default is *5* minutes.

Troubleshooting

I cannot log in with the DDP Server address or cannot access the DDP|ST Agent apps.

See Set a Screen lock option on the tablet.

An error message displays: Commercial Android multi-user capability is not supported.

Currently, only a tablet owner account is supported with Commercial Android.

My tablet is no longer paired with my original device.

Did you enroll a new device? This automatically unpairs the previous device.

DDP|ST Password Manager and DDP|ST Mobile Pairing apps no longer display.

Did you tap Uninstall on DDP|ST Agent app? If so, the other two apps are disabled and no longer display. However, your data still exists. If you run the DDP|ST Agent app and activate against the DDP Server, the other apps will display and your data will be available.

I tapped theDDP|ST Password Manager icon, but nothing displayed.

Check with your Administrator whether One-time Password is enabled for you. If not, ask if it is an option for you.

End User Experience

To use DDP|ST for Android, you must convert your consumer-mode Dell tablet to commercial mode. Your administrator will:

- Notify you that your DDP|ST for Android user account is set up
- Inform you about credentials for logon
- Send you the DDP Server address for logon
- Inform you of the length and character requirements for Password Manager's master password

Set a Screen lock option on the tablet

For enhanced security when using DDP|ST for Android, you are required to set a screen lock. Before using the DDP|ST Agent app, navigate to **Settings > Security > Screen lock** on your Dell tablet and set a pattern, PIN, or password. Otherwise, you cannot access the DDP|ST Agent apps.

Download and run the DDP|ST Agent app

To get started:

1. Download the **DDP|ST Agent** app to your tablet  .

   NOTE: Your enterprise will inform you if you should download the app from the Google Play Store or from another location.
2. In the tablet's APPS drawer, tap the **DDP|ST Agent** icon.

   The Dell Data Protection | ST Agent screen displays.
3. Tap **Agree** for the license agreement.
4. Enter the DDP Server address.
5. Enter your logon name and password, based on information from your administrator.
6. Tap **Login**.

   The tablet is now in commercial mode, and DDP|ST Agent displays these apps:

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

Enroll and pair devices

Pairing your Dell tablet with another mobile device provides recovery in case you forget your password.

- On the Dell tablet, be sure to Download and run the DDP|ST Agent app.
- On the other mobile device or smartphone, install and open the **Dell Security Tools Mobile** app  .

NOTE: Your enterprise will inform you if you should download the app from the Google Play Store or from another location.

On the mobile device or smartphone

1. Do one of these:
   - If you just installed the **Dell Security Tools** app, tap **Skip** and then tap **Get Started**. Then, create and confirm a PIN.
   - If you installed it earlier, run the **Dell Security Tools** app, enter your PIN, and tap **Sign In**.
2. At the bottom of the next screen, tap **Enroll a Computer**. (This also applies when enrolling a Dell tablet.)

A five-character alphanumeric mobile code displays on the mobile device.

On the Dell tablet

1. Tap the DDP|ST Mobile Pairing icon.

   A status message displays, *No device paired*.

   NOTE: If a message displays that One-time Password is disabled, check with your Administrator whether it can be enabled.

2. At the bottom of the screen, tap Enroll Device.
3. Enter a unique identifier for the mobile device, for example, MySmartphone. Later, if you forget your tablet password, the tablet lists this name to remind you which mobile device to use to recover access to the tablet through a one-time password.
4. In the tablet's Mobile Code field, enter the five-character alphanumeric mobile code from the mobile device/smartphone.
5. Tap Next. A pairing code displays.

On the mobile device or smartphone

1. At the bottom, tap Pair Devices.
2. Tap Manual Entry.

   NOTE: Currently, Scan QR Code is not available for the tablet.

3. Type the pairing code that displays on the Dell tablet. You do not need to type spaces.
4. Tap Done.
5. Tap Pair Devices.

   A 6- to 10-digit numeric verification code displays.

On the Dell tablet

1. Tap Next.
2. Tap the Verification Code field, and type the verification code displayed on the mobile device/smartphone.

   This 6- to 10-digit numeric code verifies that the two devices have been paired.

   NOTE: If you exceed the maximum number of retries to enter the correct code, you must restart the pairing process.

3. Tap Submit.

   In the Status field, the name of the paired mobile device displays.

On the mobile device or smartphone

1. Tap Next.

   A dialog prompts you to be sure you have completed enrollment.

2. Tap Continue.

   A green checkmark and message confirm enrollment.

3. Tap the Edit icon to enter a descriptive name for your tablet.
4. Tap Finish.

Recover your password

To recover your tablet password, you must have previously paired your Dell tablet and mobile device.

On the mobile device or smartphone

1. Run the **Dell Security Tools** app, enter your PIN, and tap **Sign In**.
   The name of the paired tablet displays.
2. At the bottom of the screen, tap the icon next to One-time Password.
   A numeric One-time Password displays.

On the Dell tablet

1. On the Sign-in screen, tap **I cannot access my account**.
   The screen lists the name that you created for the mobile device paired with this tablet.
2. In the One-time Password field, type the password that your mobile device displays.
3. Tap **Unlock**.
4. Select **Pattern**, **PIN**, or **Password**.

   NOTE: If you do not enter a new pattern, PIN, or password now, your previous forgotten password remains.
5. At the Encryption screen, select an option and tap **Continue**.
6. Enter your new password and tap **Continue**.
7. Confirm your new password and tap **OK**.
8. At the Settings screen, select your notification preference and tap **Done**.

Unpair a device

On the Dell tablet

1. On the tablet, run the **DDP|ST Agent** app.
2. Log in with the DDP Server address.
3. Tap the **DDP|ST Mobile Pairing** icon.
4. At the bottom, tap **Unpair**.
5. Tap **Continue** to confirm that you want to unpair the device.
   The Status displays, *No device paired*.

On the mobile device or smartphone

1. On the Dell Security Tools app, tap the Security Tools title bar to open the navigation drawer.
2. Tap **Remove Computers**.
3. Tap the checkbox next to the name you created for the Dell tablet.
4. At the bottom, tap **Remove**.
5. At the confirmation dialog, tap **Continue**.

Enroll a new device

When you successfully enroll a new device, the tablet is automatically unpaired with the previous mobile device.

To enroll a new device:

1. On the tablet, run the **DDP|ST Agent** app.
2. Log in with the DDP Server address.
3. Tap the **DDP|ST Mobile Pairing** icon.
4. At the bottom, tap **Enroll New Device**.
5. Tap **Continue** to confirm that you want to unpair the current mobile device and enroll a new one.
6. Continue with Enroll and pair devices.

Use DDP|ST Password Manager

Password Manager allows you to create a single master password for accessing your Password Manager account, from where you can then manage passwords used in websites, mobile applications, and network resources. With Password Manager you can:

- Create names for website categories, for example, *Email*, *Cloud Storage*, *Connectivity*, *News*, *Editors*, *Social Media*.
- Create accounts where you store user name and password credentials for websites or software applications and then use Password Manager to log on automatically.
- Modify your master password or other passwords.
- Back up and restore stored logon credentials.

Create a master password and new account

1. In the tablet's APPS drawer, tap the **DDP|ST Agent** icon  .
2. On the DDP|ST Agent screen, tap the **DDP|ST Password Manager** icon.

   The Dell Password Manager screen displays.
3. Tap the **Password** field and then enter a master password.

   NOTE: Your administrator has set requirements for length and characters.
4. Confirm the password.
5. Tap **Login**.

   The DDP|ST Password Manager screen displays.

   NOTE: Before pressing + (plus) to create a new account, the best practice is to first determine the categories that you want to use for your website accounts. See Create categories for website accounts.

Log in to DDP|ST Password Manager

1. On the DDP|ST Agent screen, tap the **DDP|ST Password Manager** icon.
2. Tap the **Password** field and then enter your master password.
3. Tap **Login**.

If you are inactive for a length of time set by your administrator, Password Manager closes and the Password login screen displays. Repeat step 2 and step 3 above.

Create categories for website accounts

When you use Password Manager to store a password for a website, it allows you to select a category for that website account. Existing categories include Favorites, Business, and Personal. Before you create a new website account, determine if you want additional categories.

To create a category for website accounts:

1. At the top, tap **All Categories** and select **New Category.**
2. Type a category name, for example, *Email*, *Cloud Storage*, *Connectivity*, *News*, *Editors*, *Social Media*.
3. At the upper right, tap **Save**.

   The new category displays in the menu.

Organize categories

1. At the top left, tap the title bar to open the navigation drawer.
2. Tap **Settings**.
3. Tap **Organize Categories**.
4. Press and hold a category row until the row is highlighted. Then drag it to a different location.

Create new website accounts

Use the Password Manager Account screen to add accounts.

To create new website accounts:

1. On the title bar, tap **+** (plus icon).

   The Password Manager Account screen displays.
2. In the Description field, enter a title or description for that account.
3. Optionally, tap the **star** icon to indicate that account as a favorite.
4. To the right, tap the category field and select a category.

   For more information, see Create categories for website accounts.
5. Tap the **Website** field and enter the website URL.
6. Tap the **Username** field and enter your user name for that website.
7. To the right of the **Password** field, tap the Password Generator icon.

   Password Manager automatically generates a password. To modify the strength of the password, see Select Password Generator settings.

   NOTE: If you enter a password instead of using the Password Generator, a slider bar indicates whether the password is Bad, Poor, Fair, Good, or Best.
8. In the upper right, tap **Save**.

   The account is added to the Password Manager main screen.

Use menu options for website accounts

After you have numerous website accounts set up, you can use the icons in the title bar to:

- Search for an account.
- Edit a website account or password, or identify it as a favorite.
- On the overflow menu, you can sort or delete an account.

Sort website accounts alphabetically or by priority

1. At the top right on the Password Manager Home screen, tap the Menu overflow icon.
2. Tap Sort By.
3. Select an alphabetical or priority option.
4. To view website accounts within one category only, select an option from the Categories menu.

Modify settings

You can modify password length and characteristics, your master password, and clipboard timeout.

To modify settings:

1. At the top left, tap the title bar to open the navigation drawer.
2. Tap Settings.

Select Password Generator settings

1. In Settings, tap Password Generator.
2. Modify password length.
3. Check a checkbox to allow uppercase, lowercase, numbers, and symbols. Clear a checkbox to prevent use.
4. In the upper right, tap Save.

Modify clipboard timeout

1. In Settings, tap Clipboard Timeout.
2. Modify the settings. Options range from *15 Seconds* to *10 Minutes*.
3. Tap Done.

Change master password

1. In Settings, tap Master Password.
2. Complete each field.
3. Tap Save in the upper right.

Back up and restore logon information in DDP|ST Password Manager

1. In the top left, tap the DDP icon to open the navigation drawer.
2. Tap Settings > Password Manager Database

   NOTE: The date of the last backup displays, if applicable.
3. Do one of these:
   - Tap Backup Password Manager Accounts and then Backup Now.
   - Tap Restore Password Manager Accounts and then Restore Now.

Sign out from DDP|ST Password Manager

1. At the top left, tap the title bar to open the navigation drawer.
2. Tap Sign Out.

Auto-update DDP|ST apps

By default, the DDP|ST Password Manager and DDP|ST Mobile Pairing apps are set to *Auto-update*.

Auto-update is a best practice, to ensure security updates are applied immediately.

To view this setting:

1. From the navigation drawer in Google Play Store, tap **My apps**.
2. Tap the **Menu overflow** icon.
3. For auto-update, ensure that the checkbox is checked.

NOTE: If one user manually updates the app, the update applies to all user accounts on that tablet, based on Android behavior.

Log out of DDP|ST Agent

1. Navigate to the **DDP|ST Agent** screen.
2. In the upper right, tap **Logout**.

Uninstall DDP|ST Agent

If you plan to use DDP|ST for Android again in the future, Dell recommends that you do **not** uninstall DDP|ST Agent.

NOTE: If you uninstall DDP|ST Agent, DDP|ST for Android is no longer in commercial mode. The DDP|ST Password Manager and Mobile Pairing apps no longer display. Your data still exists if you want to reinstall later.

To uninstall:

1. Tap **Settings > Apps**.
2. Tap the **Downloaded** tab.
3. Tap **DDP|ST Agent**.
4. Tap **Uninstall**.


0 XXXXXA0 X