imation

QUICK START GUIDE

Welcome to **Defender Collection™ Device Control + Encryption, Version 11.0** software from Imation (www.imation.com). Device Control encrypts and protects sensitive information on removable drives, such as USB flash drives and removable hard drives. Encryption is designed to prevent unauthorized access to confidential data stored on removable drives. This *Quick Start Guide* discusses how to use Device Control.

Device Control is a removable drive-installed security application that does not install on the PC. Device Control is used to encrypt and decrypt files on the removable drive itself. Device Control executes and runs from the removable drive when the user double-clicks the **OpenSecureFiles.exe** file on the drive. Since it runs from the removable drive, Device Control does not require any special PC administrative rights to run. Device Control is designed to protect information on drives that are portable, such as those used on multiple PCs. Device Control can also decrypt and open files encrypted on the removable device that have been automatically encrypted by Defender Collection Control Client software from Imation, an optional and complementary application that works with Device Control. Any new files that are encrypted with Device Control on the removable drive can also be decrypted by Control Client.

Device Control is supported on Microsoft Windows XP Home, XP Pro, Vista, and Windows 7, 32- and 64-bit versions. The software is not supported on Windows 95, Windows 98, Windows ME, Linux, or any of the Macintosh operating systems. You can encrypt any type of file supported by the Microsoft Windows operating system through Device Control.

Important Product Use Concepts

1. **If you forget both your password and recovery hint, you will not be able to access the encrypted files on the drive unless you have upgraded to the enterprise managed version**. You will need to remember either your password or your recovery hint question answer to be able to access your encrypted files. If you are concerned about forgetting your password and recovery hint, you should consider upgrading to the enterprise version of Device Control, which the Defender Collection Control Server manages. The Enterprise Edition of the software integrates with a Web-accessible server application that provides:

- Administrator password recovery for users that forget their password and recovery hint
- Audit tracking of encrypted file system content
- Dynamic revocation of authorized password access to encrypted file system content if the drive is lost/stolen and the password is compromised
- Optional enforcement of strong passwords and periodic password changes

For more information, please refer to "*Enterprise Mode*" on page 6.

2. **You can open and edit your files from within the Device Control software and any changes will be automatically saved**. Any edits you make to files that you have previously encrypted and are opening from within the Device Control application will be automatically saved and re-encrypted when you save or exit your application. If you perform a Save As operation, Device Control assumes you want to decrypt and save your changes to a location other than the drive.

I. Setting up Device Control

If your drive is set to auto-run, Device Control should auto-run whenever you insert the drive, except if your PC has the Windows 7 operating system. Windows 7 users cannot enable auto-run through their system settings because Windows 7 has disabled this functionality for removable devices. They, and any other users who do not have the auto-run functionality enabled through their Windows operating system, must double-click the **OpenSecureFiles.exe** program file on their drive every time that they want to launch the program.

The first time you run the application, you will be asked to establish your password and password recovery hint unless Control Client has automatically installed Device Control on your drive. Then, the login information you established through Control Client also applies to Device Control. You will not need to set up Device Control if Control Client has installed it on your drive.

1. Insert your drive into your PC, if it is not already inserted.
2. If the **Device Control +Encryption End User License Agreement** dialog box does not display:
   a. Navigate to the drive letter that corresponds to the removable drive with which you are working through Windows Explorer or My Computer.
   b. At the top level of the removable drive, double-click the **OpenSecureFiles.exe** program file.
3. Review the license in the **Device Control +Encryption End User License Agreement** dialog box.
4. To accept the license agreement, click **I Accept**. (If the user does not accept it, they cannot use the software.)
5. In the **Device Control +Encryption User Setup** dialog box, enter the password, hint information, and click **OK**.

   Note: The password is case-sensitive and the hint answer must be eight characters or longer.
6. The Device Control window that enables the user to perform encryption operations displays.

   Any folders or files that you drag into the window are automatically encrypted. Any folders or files that you drag out of the Device Control window are automatically decrypted. Any files that you have previously encrypted and that you double-click in the Device Control window will automatically decrypt and the software will launch the application associated with that file type (e.g., a .doc file will launch Microsoft Word).

   Note: For enterprise mode setup, in the **Device Control +Encryption Server Setup** dialog box, enter the server connection URL in the **Control Server URL** box if the URL is not already displayed and enter your email address. You will also be required to verify your email address by entering it a second time. Then, click **OK**.
   - or -
   If the server connection URL is displayed, click **OK**. If you want to learn more about enterprise mode setup and features, please refer to "*Enterprise Mode*" on page 6.

Note: The **Device Control +Encryption Server Setup** dialog box only displays during enterprise mode setup.

II. Logging into the Device Control Application

After you have set up the drive, you must log into Device Control whenever you launch it. As with setting up the drive, if your PC has the Windows 7 operating system installed or the auto-run functionality is not enabled for your operating system, you must double-click the **OpenSecureFiles.exe** file to launch the program. If the auto-run functionality is enabled for the drive, it will auto-run when you insert it into your PC.

1. Insert your drive into your PC, if it is not already inserted.
2. If the **Device Control +Encryption Login** dialog box does not display:
   a. Navigate to the drive letter that corresponds to the removable drive with which you are working through Windows Explorer or My Computer.
   b. At the root level of the removable drive, double-click the **OpenSecureFiles.exe** program file.
3. Enter your password and click **OK**.

   The Device Control window displays.

If you cannot remember your password, please refer to "*Recover password*" on page 5 for instructions on how to recover your password.

III. Encrypting Files and Folders on Your Removable Drive

The left pane of the Device Control window displays the root drive letter of your removable drive and a navigation tree of any subfolders you have created. You can create new folders and rename folders as you desire. Note that right-clicking the context menus that Windows Explorer provides is not supported.

There are several methods for encrypting files and folders: dragging-and-dropping files and/or folders into the left or right pane of the Device Control window, clicking on the **Encrypt** button in the toolbar, selecting **Encrypt** from the **File** menu in the Device Control window, saving a file to the root of the drive, or cutting and pasting files and/or folders to the root of the drive through Windows Explorer.

1. To add folders and/or files through dragging-and-dropping, open Windows Explorer, if it is not already open.
2. In Windows Explorer, select one or more files and/or folders.
3. Drag-and-drop the selected items onto a location in the Device Control window or to the root of the drive.

   – or –

1. In the Device Control window, select the folder location where you want to store the encrypted file or create a new folder and encrypt files to that location.
2. Click the toolbar button for adding files.

3. In the **Select Files for Encryption** dialog box, select one or more files to encrypt and click **Open**.

   – or –

   When you have a file open, save it directly to the root of the drive.

   – or –

   Cut-and-paste one or more files and folders to the root of the drive through Windows Explorer.

The Device Control window displays both encrypted files on the drive as well as any files that may have been copied to the drive that are not encrypted. The encryption state of the file is indicated by the "Encrypted" column in the right pane. To encrypt an unencrypted file, simply select the file in the right pane and click the **Encrypt** button on the toolbar.

IV. Decrypting Files and Folders on Your Removable Drive

When the user decrypts files through the Device Control window, Device Control decrypts the files to the user-specified location. A copy of the original encrypted files will remain in the encrypted file system until deleted. After the decryption of a file or folder, the decrypted item is not protected and can be freely used. The user can choose to decrypt files to a hard drive or networked drive as well as to removable storage media.

The user can decrypt files through the Device Control window **Decrypt** button or menu selection or by selecting the files in this window and dropping them onto a location in Windows Explorer. They must use the Device Control user interface to decrypt files. Otherwise, the files will still be encrypted.

A. Decrypt through dragging-and-dropping

1. In the left pane of the Device Control window, select the folder that contains the file (s) to decrypt and select the file (s) in the right pane.
   a. Drag-and-drop the selected items onto a folder displayed in Windows Explorer or directly to the desktop.
   b. If you have your application (e.g., Microsoft Word, Excel, PowerPoint, Media Player) open, you can also decrypt by dragging-and-dropping the file from the Device Control window directly onto the associated application. This will automatically decrypt the file and display it within the application.

B. Decrypt through the Decrypt button

1. In either pane of the Device Control window, select a folder to decrypt.
   – or –
   In the left pane of the Device Control window, select the folder that contains the file (s) to decrypt and select the file (s) in the right pane.
2. Click the toolbar button for decrypting files.
3. To decrypt a folder or multiple files, in the **Browse for Folder** dialog box, select the location for the decrypted content and click **OK**.

   – or –

   To decrypt a single file, in the file saving dialog box, select the location for the data and click **Save**.

V. Opening and Updating Encrypted Files

If the user opens an encrypted file, modifies the file, and saves it, Device Control adds the modified version to the encrypted file system and supersedes the previous version.

To open a file, double-click the file shown in the Device Control window.

– or –

Select the file and click the **Open** button on the toolbar.

As long as there is an application associated with the file type installed on the PC, the file immediately opens in the application.

Note: To add the modified version of an opened file to the encrypted file system, the user can save the changes before closing the file and application.

VI. Deleting Files

The user can delete encrypted files from the removable drive from within the Device Control window by selecting them and clicking the **Delete** icon on the toolbar or by choosing the **Delete** option from the **File** menu.

Files can also be deleted using Windows Explorer or any standard Windows method. If this is done while the Device Control window is open, the files may still be displayed in the file list until a user action is taken that causes the file list to be refreshed. In the event that a deleted file is still shown prior to a list refresh, it will be inaccessible nevertheless.

VII. Password Management

The password recovery feature enables recovering the encrypted Device Control password if it has been forgotten. After unsuccessfully trying to log in, the user can use the hint answer that they previously entered when setting up Device Control. Also, the user can modify their password and/or hint question and answer at any time from within the application.

A. Recover password

1. When trying to access the encrypted contents:

   In the **Device Control +Encryption Login** dialog box, click **Recover Password**.

   – or –

   a. Enter anything in the **Device Control +Encryption Login** dialog box and click **OK**.

   b. In the **Device Control +Encryption Login Failure** dialog box, select **Attempt password recovery** and click **OK**.

      Note: Instead of going through the password recovery process, the user can re-attempt to log in by selecting **Enter new password** and clicking **OK**. The **Device Control +Encryption Login** dialog box displays again.

2. In the **Device Control +Encryption Password Recovery** dialog box, enter the hint answer into the **Response** box and click **OK**.

3. In the **Device Control +Encryption Password Recovered** dialog box, click **OK** after noting the password.

   The **Device Control +Encryption Login** dialog box displays.

B. Modify password

1. In the Device Control window, click **Password** on the **Tools** menu.
2. In the **Change Password** dialog box, enter the existing password in the **Old Password** box.
3. Enter a new password in the **New Password** box, confirm it, and click **OK**.

C. Modify hint question and answer

1. In the Device Control window, click **Hint** on the **Tools** menu.
2. In the **Change Password Hint** dialog box, enter a new hint question and answer and click **OK**.

VIII. Enterprise Mode

When the software has been upgraded and is operating in enterprise mode, Device Control communicates with a Web-accessible Control Server application that provides advanced administrative features, including remote password administration and recovery, drive auditing features, and the ability to dynamically revoke access to the encrypted files on the drive it if is lost or stolen or if the password is compromised.

The user must be online and connected to Control Server through either a corporate network or the Internet to use Device Control for the first time in enterprise mode. The user may also be required to be online with Control Server on a periodic basis to ensure the audit trail is kept up-to-date and to communicate the need for the user to make password changes.

A. Upgrade to Enterprise mode

1. In the Device Control window, click **Upgrade** on the **Tools** menu.
2. In the **Device Control +Encryption License Upgrade** dialog box, enter the server connection URL in the **Control Server URL** box if the URL is not already displayed.
3. Enter your email address and verify it by typing it in twice in the provided fields.
4. Click **OK**.

B. View server connection information

The **About Device Control +Encryption** dialog box displays information about the connection to the corporate server and the policies for offline access to encrypted content on the drive.

IX. Copyright and Trademark Information

X. Contacting Imation

Technical Support Phone	800-351-8186
Direct Phone	651-704-6599
Email	techsupport@imation.com
Web site	www.imation.com
Address	1 Imation Way, Oakdale, Minnesota 55128