McAfee Encrypted USB Manager 3.1 Service Pack 1

www.mcafee.com

1. Purpose

This Service Pack provides a security update that protects devices from a potential security threat involving the password re-use threshold feature. You must complete the following steps to properly apply the security updates from the Service Pack.

- Install Service Pack 1
- Update custom read-only image files (if applicable)
- Update the read-only image on devices that have been issued to end users

2. Devices

The instructions in this Service Pack apply to all McAfee Encrypted USB Devices except McAfee Standard Driverless Encrypted USB. If you need to apply the security patch to a McAfee Standard Driverless Encrypted USB device, see “Updating the McAfee Standard Driverless Encrypted USB device” on page 6.

3. Installing Service Pack 1

Installing the Service Pack updates McAfee Encrypted USB Manager with the patch that fixes a potential security threat with the password re-use threshold feature. If you do not use this feature, you may not need to install the Service Pack. However, it is recommended that you install it in case you want to use this feature in the future.

The Service Pack also updates the default read-only image that comes with Manager (DefaultReadOnlyImage.pcf). If you have modified this file, you should create a backup to make sure that your changes are not overwritten.

To update the default McAfee Encrypted USB Manager read-only image file

1 From the main folder of the Service Pack double-click **Setup.exe**.
2 Follow the instructions in the install wizard.

4. Updating custom read-only image files

If you use a custom read-only image file (that is, a file you have modified from the default file—DefaultReadOnlyImage.pcf) you must update specific files on the custom image to apply the security patch.

After you update the file, all future device initialization operations must use the file that you modified to include the security update.

Note: For information about updating the read-only image for devices that have already been issued to end users, see “Updating issued devices” on page 3.

To update a custom read-only image file

1 Start McAfee Encrypted USB Manager and click **Device Initialization** on the main page.
2 In the **Other Tasks** area, click **Portable Content Manager**.
3 From the **File** menu in the Portable Content Manager, click **Open** and select the name of the custom read-only image file. Browse to the location of the file if it is not in the default **PortableContentFiles** folder.
4 From the **Action** menu, click **Explore Root**. The root directory of the read-only image displays in a file manager window. The folders in the root directory contain the files that you need to update to apply the security patch.
5 Open a file manager. Browse to the Service Pack folder and double click the **UpdatedFiles** folder.

6 Select the following file and press **CTRL+C** to copy it to the clipboard.
   - `SSDAPI.dll`

7 In the root directory of the file manager window (see step 4), press **CTRL+V** to paste the file in the **McAfee Enrypted USB** folder to replace the existing file of the same name.

8 In the **UpdatedFiles** folder (see step 5), select the `ISSDAPI.dylib` file and press **CTRL+C** to copy it to the clipboard. The `ISSDAPI.dylib` file is used only with the Mac version of McAfee Encrypted USB—Managed (the client software for the end user).

9 In the root directory of the file manager window (see step 4), press **CTRL+V** to paste the file in the following location to replace the existing file of the same name:
`.\Encrypted USB.app\Contents\Resources\components\`

10 In the **UpdatedFiles** folder, select the **Common.js** file and press **CTRL+C** to copy it to the clipboard.

11 In the root directory of the file manager window (see step 4), press **CTRL+V** to paste the file in the following location to replace the existing file of the same name:
`.\McAfee Enrypted USB\UI\Common\Scripts`

12 Close the file manager window for the root directory of the custom read-only image. On the main screen of the Portable Content Manager, from the **File** menu, click **Save** to save your changes to the custom read-only image.

Note: The Service Pack automatically updates the default read-only image file. If you modified this file, you should create a backup. You can then update the file using the following procedure “To update a custom read-only image file” to apply the security patch to the file.

5. Updating issued devices

After you update the read-only image file (see page 2), you must also update the read-only drive for devices that have been issued to end users. Updating an issued device replaces the old read-only image file with the new image that contains the security patch.

You can update each device manually by instructing the end user to bring the device to you. Once you have the device, you can update the device configuration to apply the security patch. You can also create and distribute a portable software package to end users so that they can update their own devices with the security patch (see “Creating a portable software package” on page 3).

Note: The Update Software program that end users use to update their devices, is available with only the Windows-based version of the client.

To manually update the read-only image on a device

1 On the main menu of Manager, click **Device Initialization**.

2 Click **Manage Devices**, and then click **Update Device Configuration**.

3 From the **Profile** list, select a profile that references an updated read-only image file.

5.1 Creating a portable software package

When you create the portable software package, you must specify the Image Type. The Image Type determines whether the read-only image that you add to the package is a *portable content file* (.pcf) or a *directory* of files and subfolders. It is recommended that you use the portable content file image type to update the file.

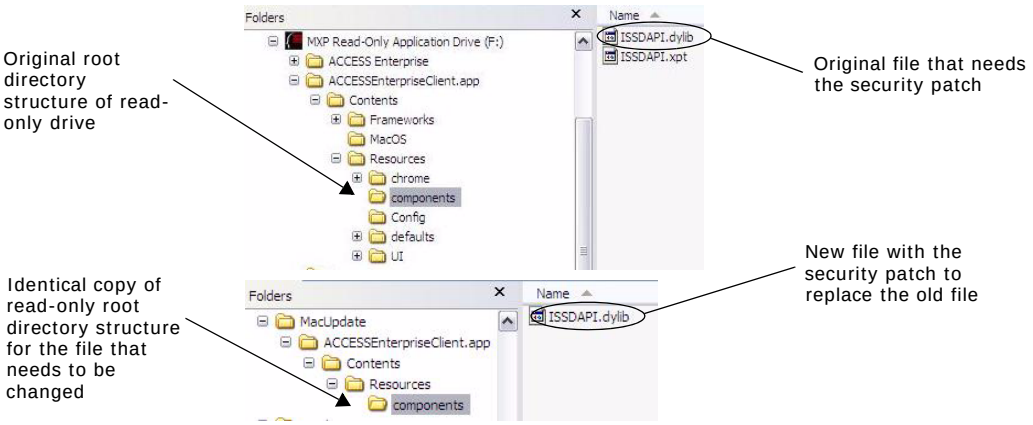
Portable content file

The portable content file is the image type that is typically used when creating a portable software package. However, this method will result in a large software update file (approximately 25 MB) as it adds the entire read-only image to the package (including the files that were updated with the Security Patch).

Directory

Use the Directory image type if you cannot distribute large files to end users. This method updates only the files on the read-only image that are affected by the security patch. However, you must create two software packages—a Mac-based version and a Windows-based version. End users must install both update packages if they use their device on Mac-based and Windows-based computers. If you initialized the issued devices with the default read-only image for Manager, you can use the directories provided with the Service Pack—PCUpdate and MacUpdate.

If you use a custom read-only image, you must create the directory. The directory must use the same file structure as the root directory of the read-only image currently on the device. That is, the folders and subfolders must use the same name and structure. The following example shows the structure of the original root directory on the read-only image. It also shows a copy of the root directory that includes the file to be updated on the read-only image. The folder that contains the patched file uses the same file structure as the root directory.



Note: If you have multiple initialization profiles, you must create a portable software package for each profile to ensure that you can update all issued devices with the security patch.

To create a portable software package from a portable content file

1. From the main menu of Manager, click **Device Initialization**.
2. In the **Other Tasks** area, click **Create Portable Software Image**.
3. Select the profile that was used to initialize the device that requires updating.
4. From the **Software Update Type** list, select **Add/Replace**.
5. From the **Image Type** list, select **Portable Content file (.pcf)**.
6. In the **Software Folder of Read-Only Image** box, click the browse button to locate the portable content file that contains the security patch. If you use the default read-only image, this file was updated when you installed the security patch for the Service Pack (see “Installing Service Pack 1” on page 2). The default read-only image file is located in the following folder: `C:\Program Files\McAfee\McAfee Encrypted USB Manager 3.1\PortableContentFiles\ (where C is the drive on which you installed Manager)`
7. In the **Software Update Package Filename** box, type a name for the portable software package file and click the browse button to set the location where you want the wizard to save the package. The default location is `C:\Program Files\McAfee\McAfee Encrypted USB Manager 3.1 (where C is the drive on which you installed Manager)`.

8 Click **Next** to create the package.

To create a portable software package from a directory

1 Follow steps 1 to 4 from the previous procedure “To create a portable software package from a portable content file” on page 4.
2 From the **Image Type** list, click **Directory**.
3 In the **Software Folder of Read-Only Image** box, click the browse button to locate the directory that contains with the files you want to add to the software package. The directory must use the same folder names and file structure as the read-only image on the device.

   If you initialized and issued devices using the default read-only image for Manager, select one of the following directory update folders included in the Service Pack folder:

   - `.\SoftwareUpdates\PCUpdate`—Windows-based version
   - `.\SoftwareUpdates\MacUpdate`—Mac-based version

   If you initialized and issued devices using a custom read-only image, select the custom directory update folder that you created.
4 In the **Software Update Package Filename** box, type a name for the portable software package file and click the browse button to set the location where you want the wizard to save the package. The default location is `C:\Program Files\McAfee\McAfee Encrypted USB Manager 3.1 (where C is the drive on which you installed Manager)`.
5 Click **Next** to create the package.

Note 1: Make sure that the read-only partition of the device has enough free space to accommodate the size of the portable update package.

Note 2: You should create a Mac-based and a Windows-based portable software package if you use the Directory image type.

5.2 Distributing the portable software package

You are responsible to distribute the portable software package(s) to end users using an appropriate method, such as sending it as an e-mail message attachment or saving the file to an accessible network folder.

5.3 Installing the portable software package

End users can install the package using the Update Software program in the client—available with the Windows-based version only. The Update Software program comes with the default read-only image. If you use a custom read-only image in which this program is disabled, the feature will not be available; end users must return the device to you to have it updated.

To install a portable software package

This procedure is typically performed by the end user.

1 In the notification area of the Windows taskbar, click the Connector icon and click **Update Software**.
2 In the **Select Update Package** box, click the browse button to locate the update package, (.upd file) and then click **Next**.
3 Follow the instructions in the install wizard.

Note: If you created a Mac-based and Windows-based portable software package, end users must install both packages to use the device with both operating systems.

6. Updating the McAfee Standard Driverless Encrypted USB device

End users must bring their McAfee Standard Driverless Encrypted USB device to you (the Administrator) so that you can apply the security patch. Before you can update a McAfee Standard Driverless Encrypted USB device, you must install the Service Pack on a computer with Manager (see “Installing Service Pack 1” on page 2).

After you install the Service Pack, you must make copies of all usage profiles used with McAfee Standard Driverless Encrypted USB devices. When you receive the device from the user, you must apply the new profile to the device. The process of applying the usage profile fixes the security issue on the device.

To create copies of a McAfee Standard Driverless Encrypted USB usage profile

1. On the main page of McAfee Encrypted USB Manager, click **Device Issuance**.
2. In the **Other Tasks** area, click **Manage Usage Profiles**.
3. Select the usage profile for the McAfee Standard Driverless Encrypted USB and click **Copy**.
4. In the **Profile Name** box, type a name for the new profile and click **Next**.
5. If multiple profiles are available to be used with McAfee Standard Driverless Encrypted USB devices, repeat steps 3 and 4 for each profile.

To update a McAfee Standard Driverless Encrypted USB device

1. Plug in the McAfee Standard Driverless Encrypted USB device to a computer with Manager (updated with Service Pack 1).
2. On the main page of Manager, click **Device Issuance**.
3. In the **Issuance Tasks** area, click **Apply New Usage Profile**.
4. Select the new profile (that you created in the “To create copies of a McAfee Standard Driverless Encrypted USB usage profile” procedure) and click **Next**.
5. Click **Finish** to complete the update, and then safely remove the device from the USB port.