



---

# ISIS Deployment Guide

**Version 5.00**

**September 14 2011**

**UG-0082**

Website

[www.plxtech.com](http://www.plxtech.com)

Technical Support

[www.plxtech.com/support](http://www.plxtech.com/support)

© PLX Technology, Inc. 2011. All Rights Reserved. The information in this document is proprietary and confidential to PLX Technology. No part of this document may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from PLX Technology.

PLX Technology provides this documentation without warranty, term or condition of any kind, either express or implied, including, but not limited to, express and implied warranties of merchantability, fitness for a particular purpose, and non-infringement. While the information contained herein is believed to be accurate, no representations or warranties of accuracy or completeness are made. In no event will PLX Technology be liable for damages arising directly or indirectly from any use of or reliance upon the information contained in this document. PLX Technology may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

PLX Technology retains the right to make changes to this product at any time, without notice. Products may have minor variations to this publication, known as errata. PLX Technology assumes no liability whatsoever, including infringement of any patent or copyright, for sale and use of PLX Technology products.

PLX Technology and the PLX logo are registered trademarks of PLX Technology, Inc.

All product names are trademarks, registered trademarks, or servicemarks of their respective owners.

Document number: UG-0082



## Contents

<b>Preface</b> .....	<b>v</b>
Pre-requisites .....	v
Related Information .....	v
Typographic Conventions .....	vi
Revision Information .....	vi
<b>Glossary</b> .....	<b>vii</b>
<b>Chapter 1 Introduction and Installation</b> .....	
Development Process and the ISIS Toolkit .....	2
Installing the ISIS Toolkit .....	3
Redistributing ISIS End User Applications .....	4
<b>Chapter 2 Using Gateway with Windows</b> .....	
Starting Gateway .....	5
Closing Gateway .....	7
Configuring a Product .....	7
Resetting a Product .....	14
Controlling Access to Data .....	15
Managing Virtual CDs .....	20
Setting Gateway Preferences .....	21
<b>Chapter 3 Using Gateway with Apple Macintosh</b> .....	
Starting Gateway .....	23
Gateway Features .....	24
Formatting Disks .....	24
<b>Chapter 4 Customizing and Deploying Gateway</b> .....	
Redistributable Gateway Files for Windows .....	26
Redistributable Files for Apple Macintosh .....	27
About the Branding File .....	27
Branding File Format .....	28
Branding for Different Languages .....	29
Changing Branding .....	30
Creating an Alternate Workflow .....	38
Creating a Gateway Installer for Windows .....	41
Creating a Gateway Package for Apple Macintosh .....	41

---

**Chapter 5 Using the Firmware Updater**

Firmware Updater Features .....	45
Starting the Firmware Updater and Updating Firmware in Windows .....	46
Closing the Firmware Updater .....	47
Resuming an Interrupted Update .....	48
Using the Firmware Updater on Apple Macintosh .....	48

**Chapter 6 Customizing and Deploying the Firmware Updater**

Windows Redistributable Files .....	50
Apple Macintosh Redistributable Files .....	51
Specifying Products and Firmware Images .....	51
Changing Branding .....	53
Branding File Format .....	54
Branding for Different Languages .....	58
Creating a Firmware Updater Package for Windows .....	59
Creating a Firmware Updater Package for Apple Macintosh .....	59

**Chapter 7 Creating a RemoteComms Driver Layer for Apple Macintosh**

This guide gives instructions on using end user applications in the ISIS toolkit version 2.3 that are for use with products based on the following PLX Technology devices:

- OXU310x
- OXU311x
- Gateway only: OXU310x or OXU311x combined with OXUFS944SE to form a USB 3.0/FireWire combi product

The guide describes how to modify the end user applications and prepare them for distribution with your products.

This guide assumes that readers are engineers who are experienced in developing storage products.

## Pre-requisites

To follow the instructions in this guide, you must have:

- One of:
  - PC with Windows XP, Vista or 7 (32 or 64 bit)
  - Intel-based Apple Macintosh with OS 10.4, 10.5, 10.6 or 10.7 (32- or 64-bit)
- One or more PLX Technology OXU310x or OXU311x devices
- Knowledge of XML

This guide assumes that you know how to use Windows facilities such as the Disk Management and Device Manager tools, and Apple Macintosh facilities.

## Related Information

The following documents offer further detail about topics covered in this guide:

UG-0081	<i>ISIS User Guide for Engineers</i>
GS-0099	<i>Getting Started with the OXU3100 Evaluation Board</i>
GS-0103	<i>Getting Started with the OXU3101 Evaluation Board</i>
GS-0101	<i>Getting Started with the OXU3102 Evaluation Board</i>
GS-0106	<i>Getting Started with the OXU3110 Evaluation Board</i>
GS-0107	<i>Getting Started with the OXU3111 Evaluation Board</i>

## Typographic Conventions

In this document, the following conventions apply.

Convention	Meaning
<i>Italic Letters With Initial Capital Letters</i>	A cross-reference to another publication
Title	A cross-reference to another section within the document
1, 2, 3	A numbered list where the order of list items is significant
■	A list where the order of items is not significant
⚡	Significant additional information
Courier	Software code
<b>Bold</b>	Significant names, for example of files or directories Text you type

## Revision Information

The following table documents the revisions of this guide.

Version	Date	Modification
5.00	September 14 2011	Updated Chapter 2 <a href="#">Using Gateway with Windows</a> , Chapter 3 <a href="#">Using Gateway with Apple Macintosh</a> , Chapter 4 <a href="#">Customizing and Deploying Gateway, Using the Firmware Updater on Apple Macintosh</a> and <a href="#">Specifying Products and Firmware Images</a>
4.00	July 05 2011	Includes Apple Macintosh information
3.00	April 07 2011	Includes OXU311x devices
2.00	December 14 2010	Updated interface and branding files format
1.00	September 20 2010	First publication



Term	Meaning
device	A PLX Technology microchip used in your products
Firmware Updater	Part of the ISIS toolkit that enables you to manage and upload firmware information for a flash device
Flash Editor	Part of the ISIS toolkit that enables you to manage flash devices, manage flash image files and load files on flash devices
Gateway	Part of the ISIS toolkit that enables you to develop an end user interface for your product
host	A PC or Apple Macintosh on which the ISIS toolkit, and other development tools, are installed for interfacing with products in evaluation, development or production
ISIS toolkit	A set of tools used in developing a product based on a PLX Technology device, part of which can be packaged for inclusion in the final product. Comprises the Flash Editor, Virtual CD Updater, Firmware Updater, Gateway and Production Programmer
ISO image	A file of the contents of a CD, which runs in the same way as a physical CD or may be placed on a physical CD, to present information to an end user
lock, unlock	Ensure that the end user is permitted to access data on the device or product hard disk, for example using password protection
product	The item you are designing and building for sale to end users, based on a PLX Technology device. Includes components such as the PLX Technology device, associated flash device and associated hard disk(s)
Production Programmer	Part of the ISIS toolkit that enables you to load flash image files on your products ready for testing or sale
Virtual CD Updater	Part of the ISIS toolkit that enables you to put a CD ISO image on your product, which is presented to an end user when they start up your product

This page is intentionally blank



## Introduction and Installation

The ISIS toolkit contains a set of utilities used when developing and producing products based on PLX Technology OXU310x or OXU311x devices.

This guide describes:

- Installing the ISIS toolkit on a host:
  - On a Windows host PC, you can install just the tools you need or the whole toolkit
  - On an Intel-based Apple Macintosh host, you install the Firmware Updater and Gateway applications

Software and instructions are different for Windows and Macintosh hosts. For details, see [Installing the ISIS toolkit on a Windows host PC](#) on page 3 and [Installing the ISIS Firmware Updater or Gateway on an Apple Macintosh host](#) on page 3

- **Gateway**—enables you to set up an end user application for:
  - Locking and unlocking your product
  - Changing configuration settings for your product

You can redistribute Gateway after you customize it with your branding and product capabilities.

For more information, see Chapter 2 [Using Gateway with Windows](#) and Chapter 4 [Customizing and Deploying Gateway](#)

- **Firmware Updater**—enables you to send firmware updates to end users.

You can redistribute the Firmware Updater after you customize it for your branding and product capabilities.

For more information, see Chapter 5 [Using the Firmware Updater](#) and Chapter 6 [Customizing and Deploying the Firmware Updater](#)

For more information on redistributing, see [Redistributing ISIS End User Applications](#) on page 4.

There are other tools in the kit, which are used at other stages of product development. The following table describes further uses of the ISIS toolkit.

To learn how to...	See	ISIS tool
Manage the firmware and configuration information on a flash device	UG-0081: <i>ISIS User Guide for Engineers</i>	Flash Editor
Update flash device content in a production environment	UG-0081: <i>ISIS User Guide for Engineers</i>	Production Programmer
Place a CD ISO image on your product's hard disk	The relevant evaluation kit getting started for your device	Virtual CD Updater

## Development Process and the ISIS Toolkit

The following table describes the recommended workflow when developing a product using PLX Technology OXU310x or OXU311x devices and the ISIS toolkit.

Step	Tool	Document
Evaluating the PLX Technology device: <ul style="list-style-type: none"> <li>Evaluate different configuration options</li> <li>Unlock the device</li> </ul>	Gateway	Relevant evaluation kit getting started guide for your device
<ul style="list-style-type: none"> <li>Upload ISO images</li> </ul>	Virtual CD Updater	
Developing your product: <ul style="list-style-type: none"> <li>Select the flash device to match the development hardware</li> <li>Upload custom firmware</li> <li>Configure device settings</li> </ul>	Flash Editor	UG-0081: <i>ISIS User Guide for Engineers</i>
<ul style="list-style-type: none"> <li>Upload ISO images</li> </ul>	Virtual CD Updater	
Configuring flash devices: <ul style="list-style-type: none"> <li>Prepare flash image content for your product</li> </ul>	Flash Editor	UG-0081: <i>ISIS User Guide for Engineers</i>
<ul style="list-style-type: none"> <li>Upload flash image content to your finished product</li> </ul>	Production Programmer	
Configuring ROM devices: <ul style="list-style-type: none"> <li>Prepare configuration and ROM patch to be stored on your product's disk</li> </ul>	Flash Editor	UG-0081: <i>ISIS User Guide for Engineers</i>
<ul style="list-style-type: none"> <li>Store configuration and ROM patch on your finished product</li> </ul>	Production Programmer	
Create scripts to automate the device configuration process	ISIS command line	UG-0081: <i>ISIS User Guide for Engineers</i>
Preparing end user applications: <ul style="list-style-type: none"> <li>Prepare end user application for updating firmware</li> </ul>	Firmware Updater	This guide
<ul style="list-style-type: none"> <li>Prepare end user application for configuring your product</li> </ul>	Gateway	

## Installing the ISIS Toolkit

This section describes how to install the ISIS toolkit on your host. On a Windows host, you can install just the tools you want or all the tools in the ISIS toolkit. On an Apple Macintosh host, you can install the ISIS Firmware Updater and Gateway.

### Installing the ISIS toolkit on a Windows host PC

These instructions assume that the installation CD is mounted as drive D:.

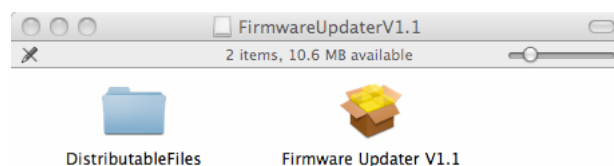
To install the ISIS toolkit on a Windows host:

1. Navigate to and double-click  
**D:\Windows\ISIS\ISISInstaller\_<x32/x64>\_vw\_xx\_yyyy\_zzzz**  
where:
  - x32/x64 is 32-bit or 64-bit, depending on your operating system
  - w, x, y and z represent the version of the software
2. Follow the installation wizard instructions. When prompted, select the tools you want to install. The default is to install all tools in the ISIS toolkit. To follow the instructions in this guide, you need to install all tools
3. To start an ISIS tool or access a redistributable end user application, go to **Start - PLX Technology - ISIS** and click the one you want.

### Installing the ISIS Firmware Updater or Gateway on an Apple Macintosh host

To install the ISIS Firmware Updater or Gateway on an Apple Macintosh host:

1. On the installation CD, navigate to the **Mac\ISIS** folder.
2. Double-click either FirmwareUpdater\_vw\_xx\_yyyy\_zzzz.dmg or Gateway\_vw\_xx\_yyyy\_zzzz.dmg as required, where w, x, y and z represent the version of the software. The relevant package installer is shown; for example:



3. Double-click the package installer. Follow the installation wizard instructions. When the installation is complete, restart your system.
4. To run the tools, go to:
  - Utilities - Firmware Updater
  - Applications - Gateway

- 5 You can customize and brand the features of the Firmware Updater and Gateway for redistribution in your own package (see [Redistributing ISIS End User Applications](#) on page 4). To do so, copy the **DistributableFiles** folder from the dmg file into a local folder on your Apple Macintosh. This contains all the files you need to modify and create a new package file.

For more information on customizing and branding, see Chapter 4 [Customizing and Deploying Gateway](#) and Chapter 6 [Customizing and Deploying the Firmware Updater](#).

- 6 Depending on your device configuration, you may need to create a custom RemoteComms driver layer. To find out if you do need to do this, see Chapter 4 [Customizing and Deploying Gateway](#) or Chapter 6 [Customizing and Deploying the Firmware Updater](#).

To create a custom RemoteComms driver layer, copy the file **MyCompanyName\_RemoteCommsSample\_Vw\_xx\_yyyy\_zzzz.zip** from the CD to a local folder on your Apple Macintosh. Follow the instructions in Chapter 7 [Creating a RemoteComms Driver Layer for Apple Macintosh](#).



To ensure that the latest USB descriptors are written to the flash device when you are upgrading from a previous version of the ISIS toolkit or using hardware programmed using a previous version of the ISIS toolkit, we advise you to reset the device configuration. To do so, use the Flash Editor; for instructions see UG-0081: *ISIS User Guide For Engineers*.

## Redistributing ISIS End User Applications

You can redistribute Gateway and the Firmware Updater to your end users. You must customize them with your branding and the features you want your end users to have.

The terms and conditions for redistributing Gateway and Firmware Updater are covered by the license agreement, which is displayed when you install the ISIS toolkit. You can view the license at any time: to do so, go to the ISIS installation folder (in Windows, usually **C:\Program Files\PLX Technology\ISIS**) and open **IsisSLA.rtf**.

You must supply any user guides you want to give your end users.

## Using Gateway with Windows

Gateway enables end users to change configuration settings for your product and to control access to data stored on your product.

You can redistribute Gateway to your end users after you customize it to match your company branding and the features you want to give end users access to. This chapter describes Gateway as supplied. For instructions on rebranding, see Chapter 4 [Customizing and Deploying Gateway](#).

This chapter includes:

- [Starting Gateway](#) on page 5
- [Closing Gateway](#) on page 7
- [Configuring a Product](#) on page 7
- [Resetting a Product](#) on page 14
- [Controlling Access to Data](#) on page 15
- [Managing Virtual CDs](#) on page 20
- [Setting Gateway Preferences](#) on page 21

### Starting Gateway

To start Gateway, go to your **Start** menu and select **PLX Technology - ISIS Tools - Gateway**. If no product is attached, the Preferences window is shown.




Until you attach a product, you can only set how you want Gateway to work; see [Setting Gateway Preferences](#) on page 21.

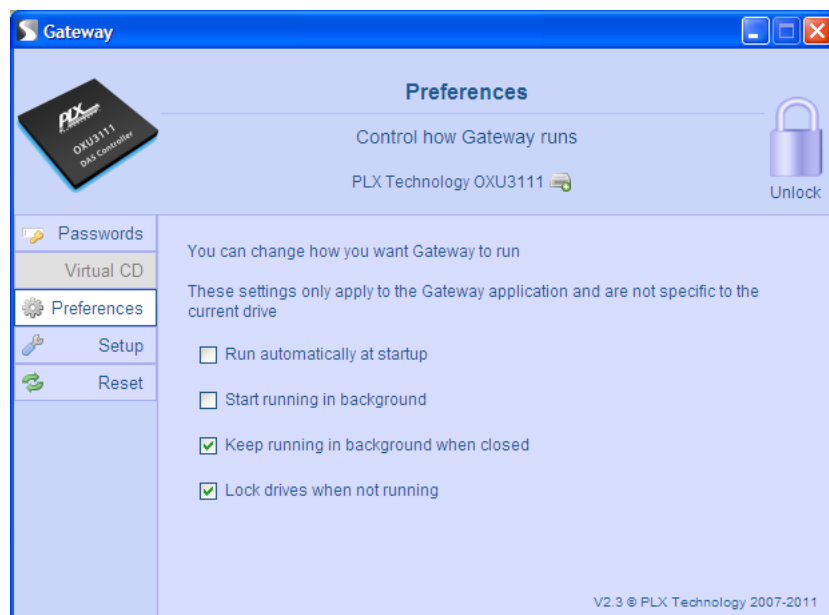
When you start Gateway with a product attached, one of the following is shown:


- If an encrypted product with a password is attached, the Lock/Unlock window is shown.




You can:

- Unlock the product by entering the password and clicking **Unlock**
  - If the product is already unlocked, you can lock it by clicking **Lock**
  - Go to the Settings window by clicking  **Settings** (see the next list item)
- If an unencrypted product or an encrypted product with no passwords is attached, the Settings window is shown, usually with the Preferences tab selected.



If two or more products are attached, there is a  **Drive** icon next to the product name. To choose the product you want, click the icon and select the one you want from the displayed list.

You can:

- ❑ Lock or unlock a product by clicking  **Lock/Unlock** to go to the Lock/Unlock window
- ❑ Select the **Passwords** tab to manage passwords for locking and unlocking access to data on the product. You can set up to 10 passwords.  
For more information, see [Controlling Access to Data](#) on page 15
- ❑ Select the **Virtual CD** tab to show, hide or remove a virtual CD presented by your product.  
For more information, see [Managing Virtual CDs](#) on page 20
- ❑ Select the **Preferences** tab to set up Gateway itself.  
For more information, see [Setting Gateway Preferences](#) on page 21
- ❑ Select the **Setup** tab to change configuration settings for your product.  
For more information, see [Configuring a Product](#) on page 7
- ❑ Select the **Reset** tab to reset the product to default settings.  
For more information, see [Resetting a Product](#) on page 14

## Closing Gateway

To close Gateway click **X** (Windows Close button) in the top right of the window. Ensure you save any unsaved changes before closing.


## Configuring a Product

To select and change configuration settings for your product, you use the Settings window Setup tab to start the drive setup wizard.

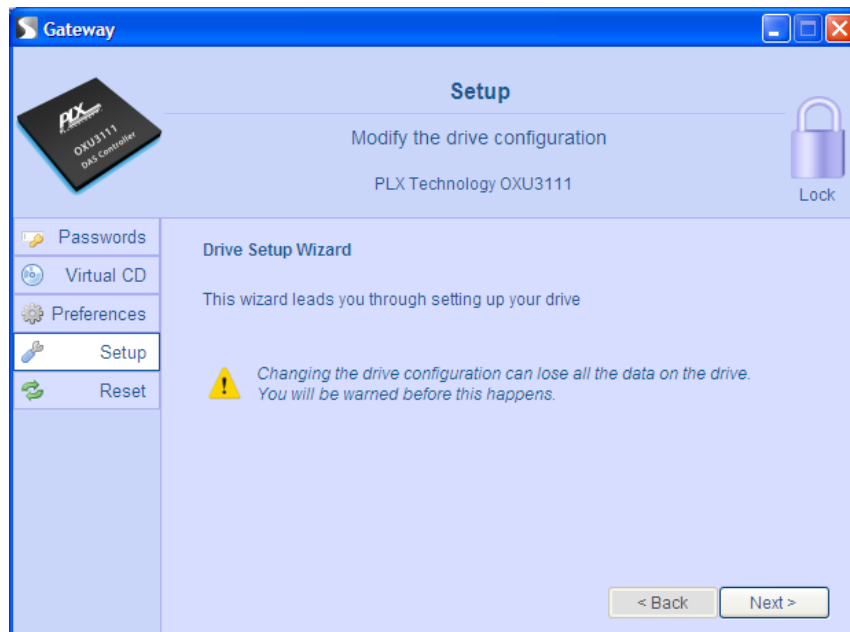
The drive setup wizard only shows the configuration settings relevant for your product. This section describes all the configuration settings available in the drive setup wizard. You use the drive setup wizard for:

- [Selecting RAID mode](#)
- [Selecting encryption settings](#)—must be enabled for password access control
- [Selecting miscellaneous settings](#), such as auto power and disk capacity
- [Setting an initial password](#)
- [Applying settings](#)
- [Formatting hard disk drives](#)

Many configuration setting changes cause any passwords and data on the disk to be lost.

Before running the wizard when you have two or more products attached, ensure you use the  **Drive** icon next to the product name to choose the product you want.

To start the drive setup wizard, in the Settings window, click **Setup**. The drive setup introduction window is shown. This warns you that changing configuration settings can cause loss of passwords and data.

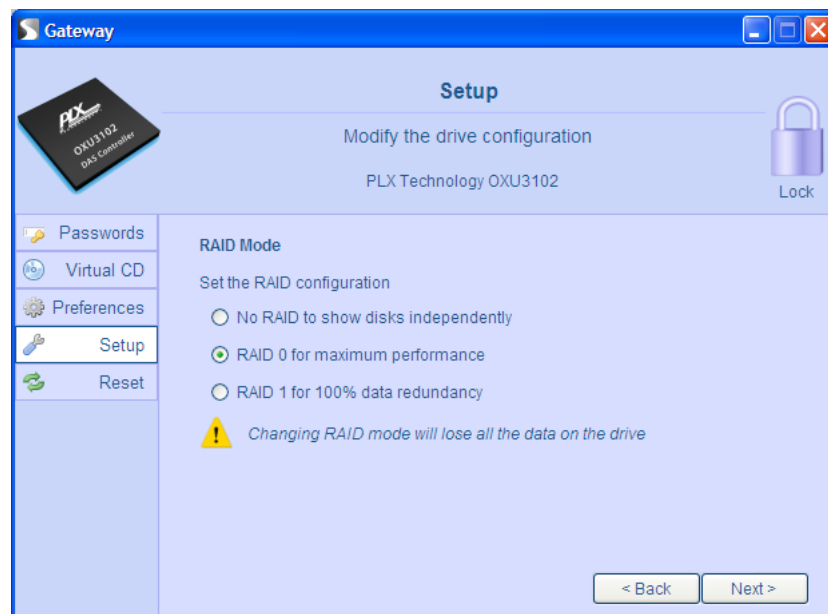


While using the wizard, click **Next** or **Back** as needed to move between windows.

The following sections describe the configuration settings in the wizard.

### Selecting RAID mode

The RAID Mode window is only shown if you have two or more hard disk drives in your product.





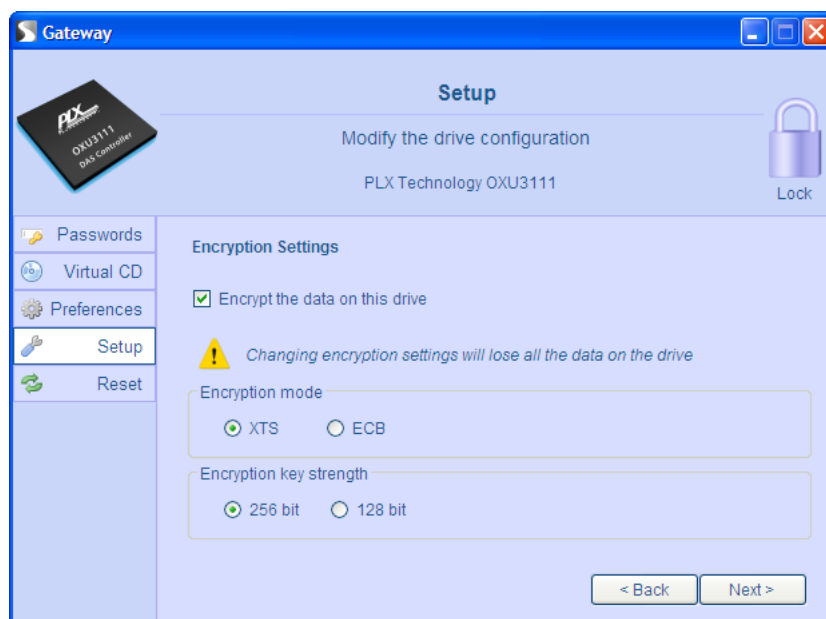
Select one of:

- No RAID—to see each hard disk drive independently
- RAID 0—to use all hard disk drives as one volume; this gives the best performance
- RAID 1—to duplicate data from one hard disk drive on to another

If you change the setting, you must reformat your hard disks once you have finished these steps.

## Selecting encryption settings

The Encryption Settings window is only shown if your product supports encryption. Not all encryption modes are available for all devices.

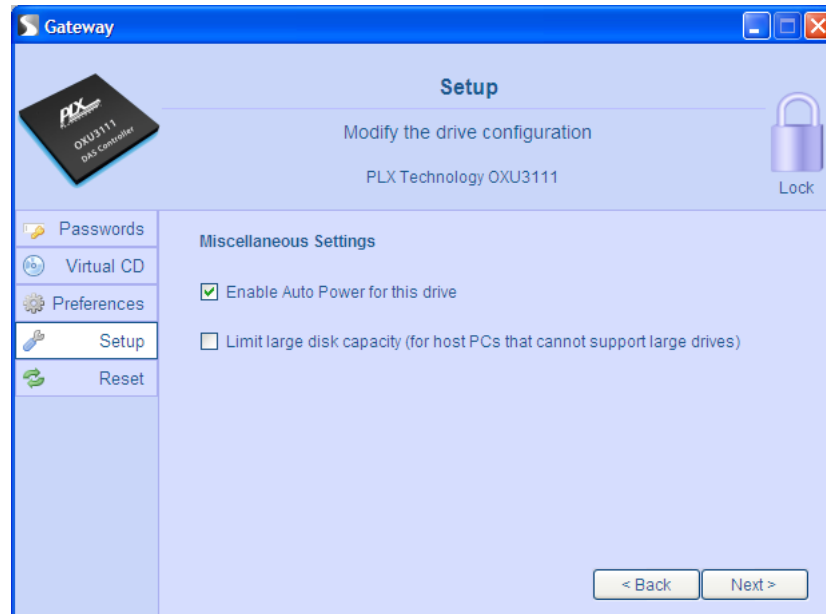


Select:

- Encrypt your data—check to enable data encryption and password access control, or leave unchecked if you do not want to encrypt your data or protect access using passwords. If you check this box, you must also select an encryption mode and encryption key strength on this tab
- Encryption mode—the encryption algorithm to use, if you checked the Encrypt your data check box
- Encryption key strength—the complexity of encryption, if you checked the Encrypt your data check box

## Selecting miscellaneous settings

You use the Miscellaneous Settings window to enable/disable auto power and large disks.

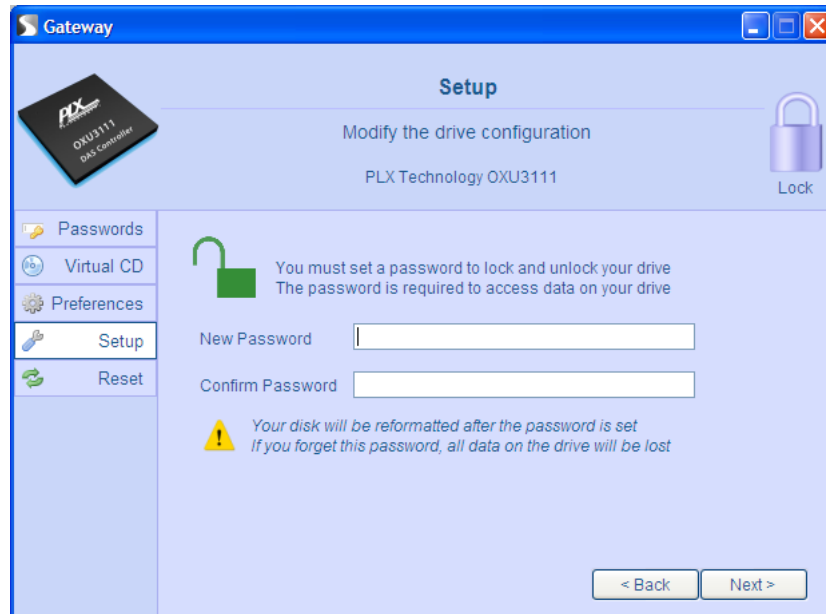


Select:

- Enable Auto Power for this device—check to enable the product to automatically reduce power consumption when not in use
- Limit large disk capacity—check if your PC does not support hard disks with 32-bit addressing, which limits disk sizes to 2.2TB. The hard disk presents a smaller size, so that it falls in the 32-bit addressing range

## Setting an initial password

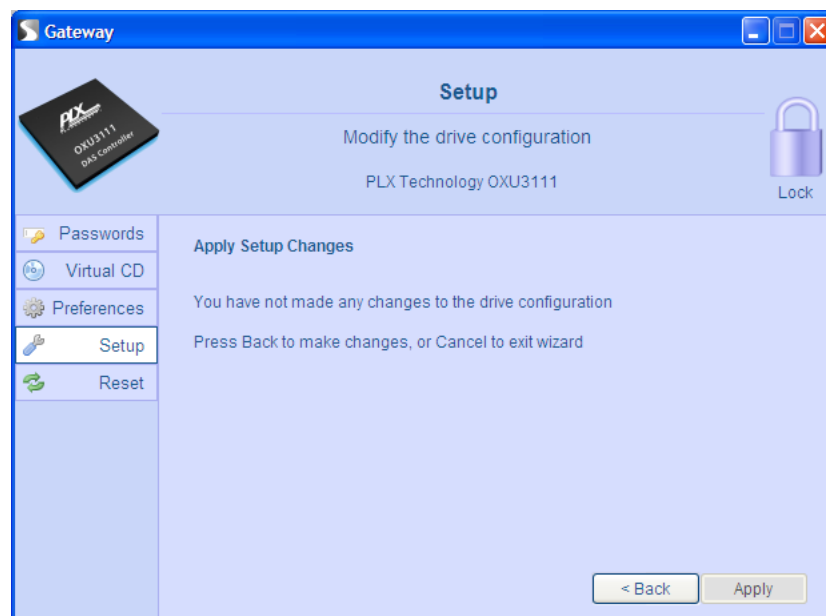
If encryption is enabled and the changes you selected cause existing passwords to be lost, you are prompted to set your initial password.



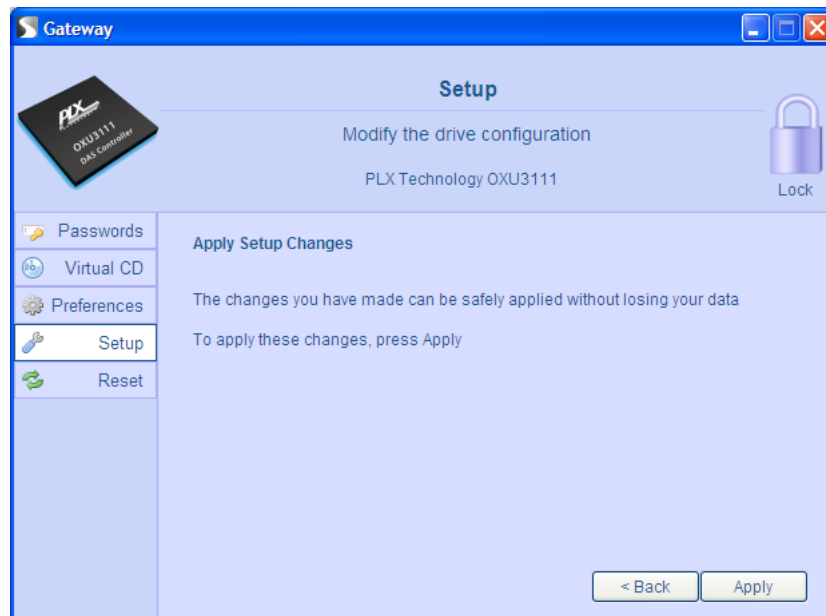
Enter a password then re-enter it. The passwords must match before you can click **Next**.

## Applying settings

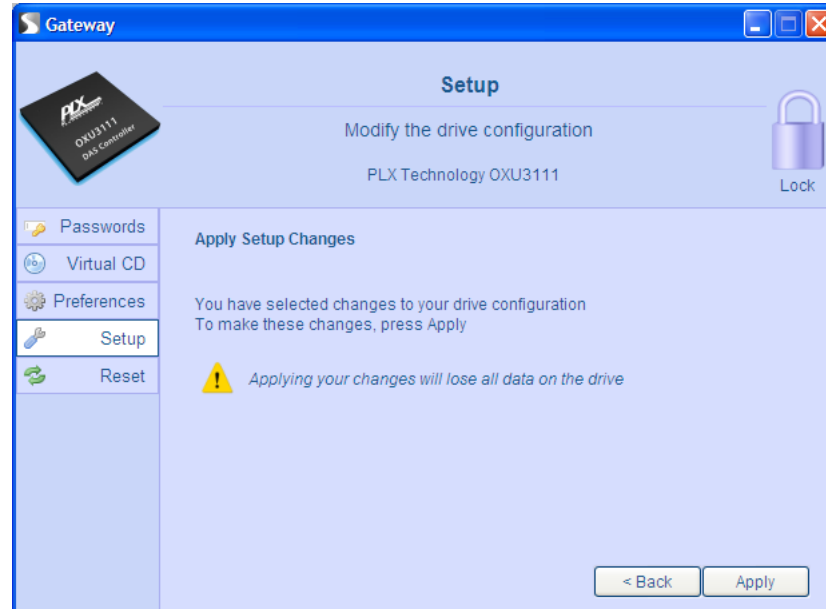
If you have made no changes, you are given the option to click **Back** to make changes, or **Cancel** to close the drive setup wizard, as follows:



If you have made changes to the configuration that do not lose the data on your disk, the window shows the following message. Click **Apply** to apply the changes; the drive setup wizard completes and closes



If you have made changes to the configuration that lose all the data on the disk and require the device to be reformatted, the window shows the following message. Click **Apply** to apply the changes



## Formatting hard disk drives

If you choose settings that cause the data on the hard disks to be lost, the hard disk must be reformatted.

If you have a single disk, RAID0 or RAID1, Gateway automatically partitions and formats the hard disk immediately after you apply the changes. A message indicating progress is shown while the hard disk is reformatted




Gateway creates a single primary partition, formatted using NTFS file system. This operation requires administrator privileges. You may be prompted by Windows to accept this, depending on the version and configuration of your Windows operating system. The following table shows the partition schemes used when creating disk partitions.

Operating system	Disk size	Partition scheme
Windows Vista or later	Less than 2.2TB	MBR
Windows Vista or later	Greater than 2.2TB	GPT
Windows XP	Any. Note that to access a disk capacity greater than 2.2TB you must use a disk with 4K sectors	MBR

If you have configured a RAID device to show the disks independently, Gateway runs the Windows Disk Management utility to enable you to manage these independent drives yourself.

## Resetting a Product

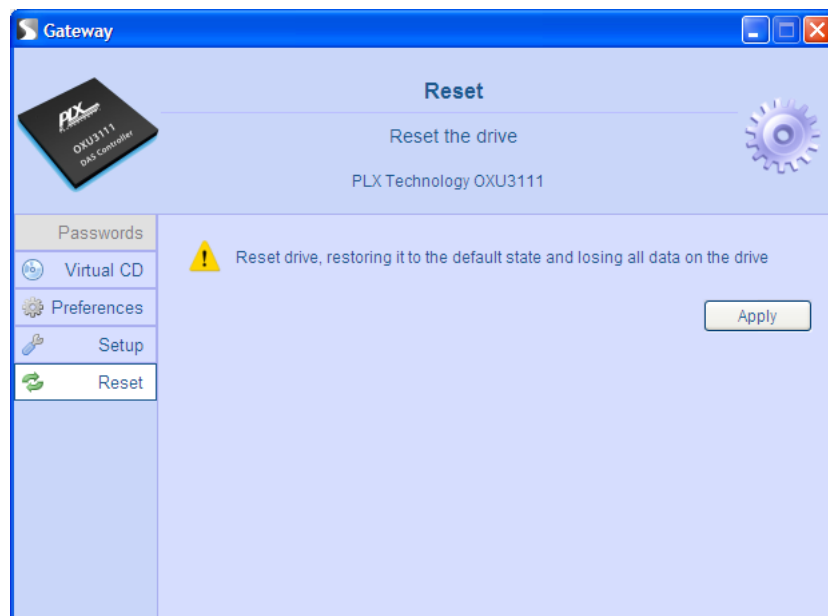
You can restore configuration settings to the original state. All data and passwords are lost when you do this.

Before resetting a product when you have two or more products attached, ensure you use the  **Drive** icon next to the product name to choose the product you want.

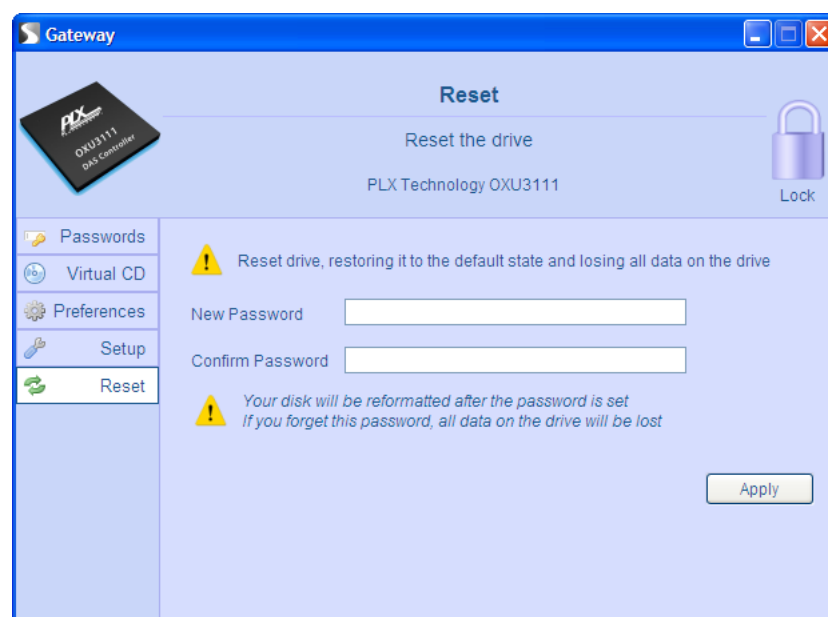
To reset configuration settings:

- 1 In the Settings window, click the Reset tab to select it. One of the following is shown:

- ☐ For a product without encryption:



- ☐ For a product with encryption enabled, you can specify a new initial password as part of the reset operation:



- 2 Click **Apply**. A message is shown warning you that you will lose your data and passwords. The drive is automatically reformatted on completion.

## Controlling Access to Data

On products that support encryption and drive locking, you can set up passwords to ensure only authorized people can access the data. Anyone entering a valid password can access all the data on all the hard disks in your product: you cannot apply a password to a specific partition in the product.

To control access to data and enable the Unlock/Lock tab, you must do the following using the drive setup wizard (see [Configuring a Product](#) on page 7):


- Enable encryption
- Set an initial password

Once encryption is enabled and at least one password is in place, the product automatically locks if the PC goes into a lower power state (for example, suspend).

You can have up to ten passwords on one product. Passwords must be 6 to 32 characters long.


This section describes:

- [Locking and Unlocking a Product](#)
- [Managing Passwords](#)

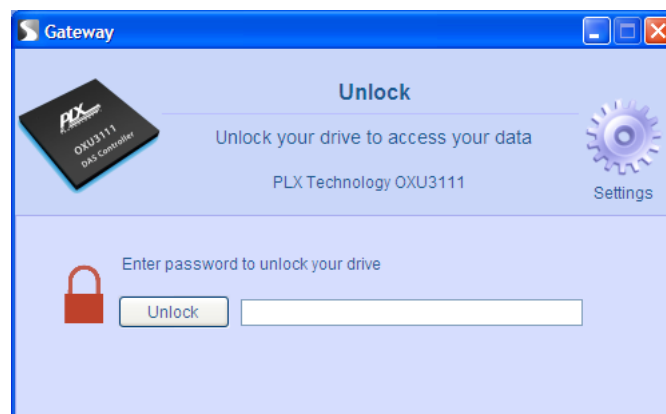
Before doing anything described in this section when you have two or more products attached, ensure you use the  **Drive** icon next to the product name to choose the product you want.

## Locking and Unlocking a Product

You can prevent unauthorized people from accessing data on your product by locking it using password access control. You do so using the Lock/Unlock window, which is shown when:

- You start Gateway with an encrypted product attached
- You are in the Settings window and click  **Lock/Unlock**.

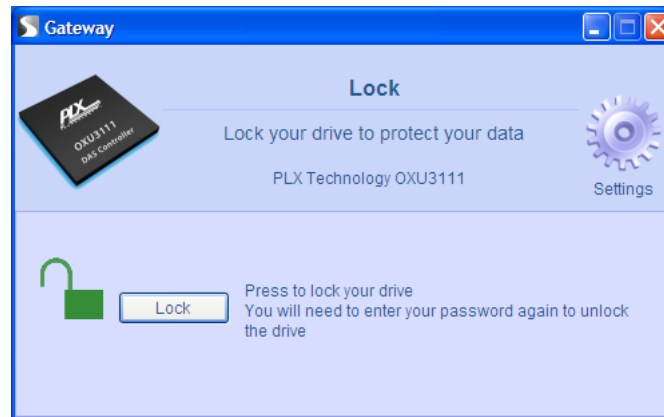
For a locked product, the following window is shown.



To unlock a product:

- 1 In **Enter password**, enter a valid password.
- 2 Click **Unlock** or press Enter. The product is unlocked and the Unlock button becomes a **Lock** button.

For an unlocked product, the following window is shown.



To lock a product click **Lock**. The product is locked and the Lock button becomes an **Unlock** button.

## Managing Passwords

You can specify up to 10 passwords on one product. All passwords give full access to all data on the product. Passwords must be 6 to 32 characters long.

You cannot delete all passwords: one password must remain. To remove password access control, you must disable encryption. For instructions, see [Configuring a Product](#) on page 7.

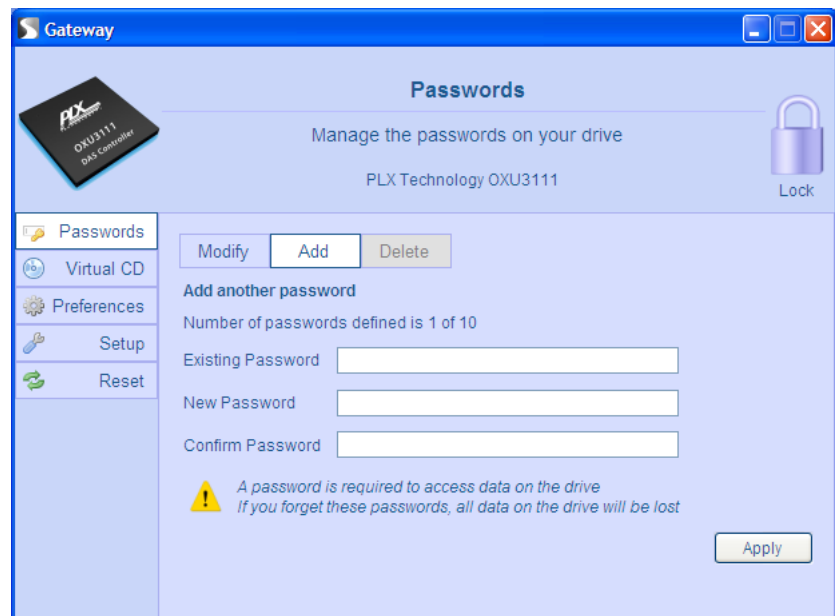
When managing passwords, you do not need to unlock the product. However, you must know an existing password.



## Adding a password

To add a password:

- 1 In the Settings window, click the Passwords tab to select it, then click **Add**.

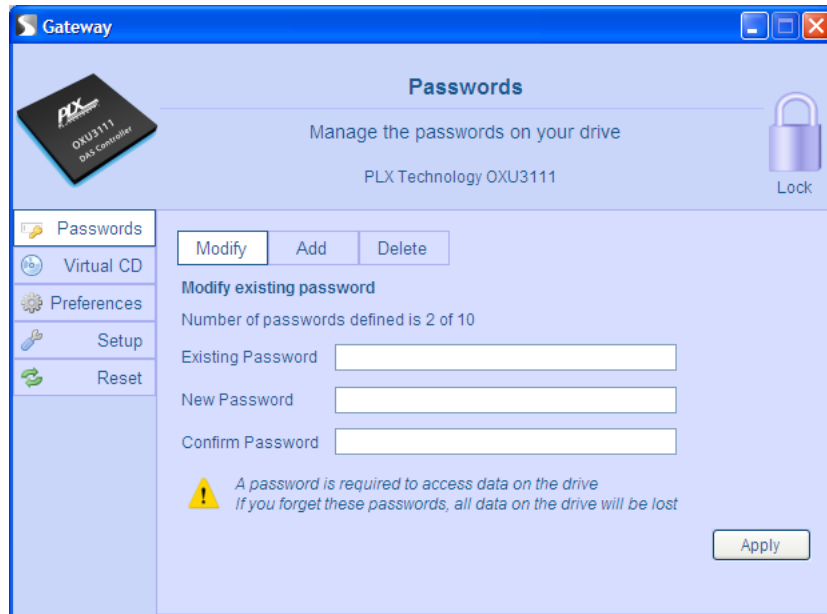


- 2 In **Existing Password**, enter a password that already works.
- 3 In **New Password**, enter the password you want to add, then re-enter it in **Confirm Password**.
- 4 Click **Apply**. The new password is stored.

## Modifying a password

To modify a password:

- 1 In the Settings window, click the Passwords tab to select it, then click **Modify**.



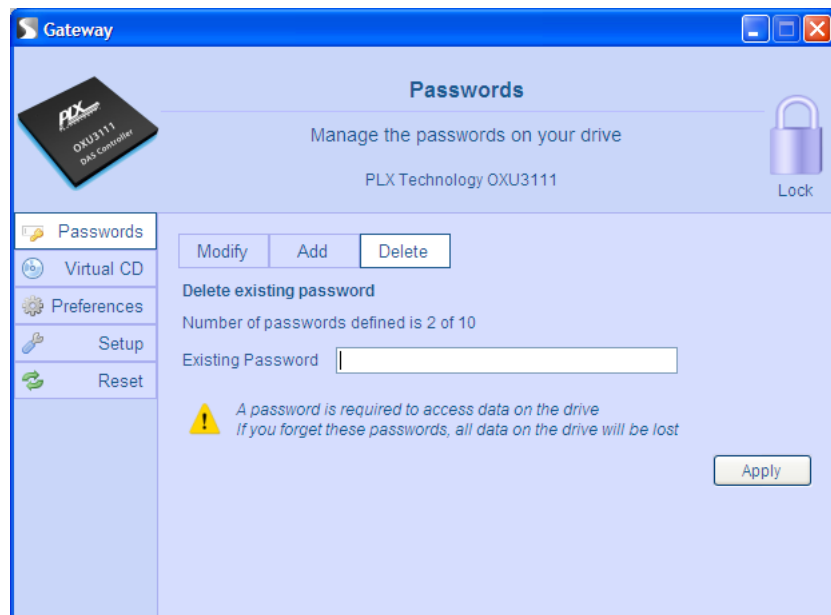
- 2 In **Existing Password**, enter the password that you want to change.
- 3 In **New Password**, enter the password you want to change to, then re-enter it in **Confirm Password**.
- 4 Click **Apply**. The password is changed.

## Deleting a password

You cannot delete all passwords: one password must remain. To remove password access control, you must disable encryption. For instructions, see [Configuring a Product](#) on page 7.

To delete a password:

- 1 In the Settings window, click the Passwords tab to select it, then click **Delete**.




- 2 In **Existing Password**, enter the password that you want to delete. A message is shown asking you to confirm the deletion.
- 3 Click **Apply**. The password is deleted.

## Managing Virtual CDs

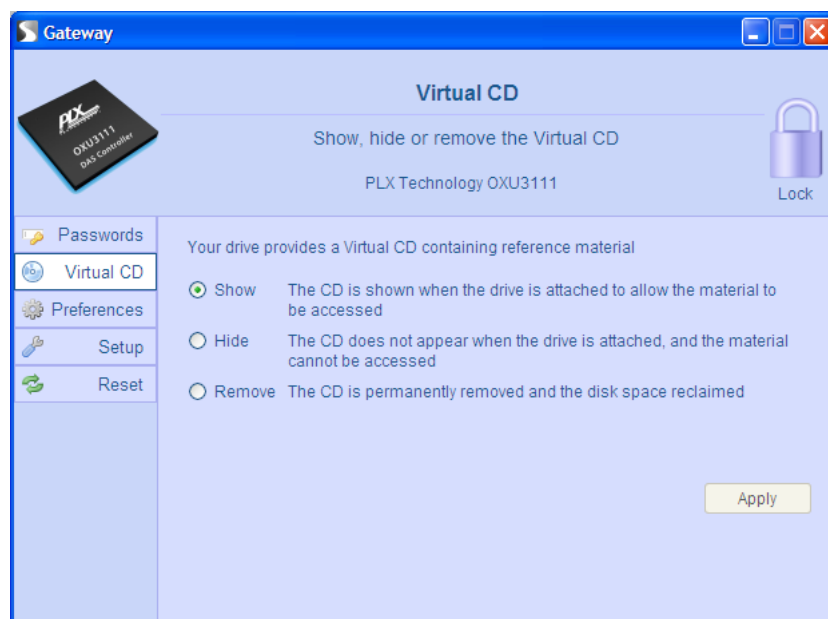
A virtual CD usually contains support software and documentation for your product.

The presence of the virtual CD can impact performance levels of the hard disk on your product, particularly for USB 3.0 devices supporting UAS.

Before changing virtual CD settings when you have two or more products attached, ensure you use the  **Drive** icon next to the product name to choose the product you want.

You can show or hide the virtual CD any time. You can also remove the virtual CD and recover the disk space. To do so:


- 1 In the Settings window, click the Virtual CD tab to select it.



- 2 Do one of the following:
  - ☐ To show the virtual CD, click **Show**
  - ☐ To hide the virtual CD, click **Hide**. If you connect the device to another PC and want to view the virtual CD, you must show it again first
  - ☐ To remove the virtual CD from the disk permanently, click **Remove**. Any data on the disk is lost and the disk is automatically reformatted
- 3 Click **Apply**. The change is saved and the Apply button is disabled.

## Setting Gateway Preferences

You can specify how Gateway runs. To do so:

- 1 Start Gateway (see [Starting Gateway](#) on page 5). If the Preferences window is not shown, click  **Settings** then click the Settings window Preferences tab.
- 2 Select any or all of the following:

Option	Description
Run automatically at startup	To start Gateway whenever you start up your PC
Start running in background	To minimize Gateway to an icon in the system tray when started manually or automatically. To open the Gateway main window, you must click the Gateway icon in the system tray
Keep running in background when closed	To minimize Gateway to an icon in the system tray when you click X (Windows close button)
Lock drives when not running	To lock any attached products when you close Gateway. If you want attached unlocked products to remain unlocked when you close Gateway (so that you can still access data on the product), leave this checkbox blank

This page is intentionally blank

## Using Gateway with Apple Macintosh

Gateway on an Apple Macintosh is functionally the same as Gateway in Windows. For full details on the functionality provided, see Chapter 2 [Using Gateway with Windows](#).

This chapter gives details of any specific differences in application appearance or features.

This chapter includes:

- [Starting Gateway](#)
- [Gateway Features](#)
- [Formatting Disks](#)

### Starting Gateway

To run Gateway, go to the Applications folder on your Apple Macintosh. The Gateway Preferences window is shown.



As with the Windows version, until you attach a product, you can only set how you want Gateway to work; see [Setting Gateway Preferences](#) on page 21.

Note that on an Apple Macintosh, the option to run automatically at startup is not available from within the application. To make Gateway run at startup:

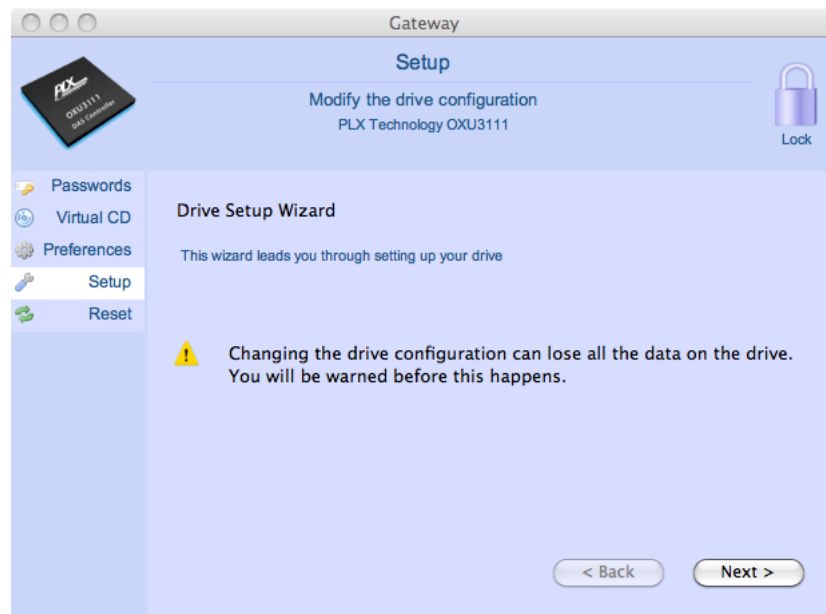
- 1 Open System Preferences and select Accounts.
- 2 Click the Login Items tab and add Gateway to this.

## Gateway Features

The majority of Gateway features on an Apple Macintosh are identical to their Windows equivalents. For example, to unlock a drive the Lock/Unlock window is shown.



To change settings, use the Setup window.



## Formatting Disks

The Apple Macintosh Gateway automatically partitions and formats the hard disk when needed, in the same way as the Windows version. However, the Apple Macintosh automatically uses APM partitions and formats the disk using the Journaled HFS+ file system.



## Customizing and Deploying Gateway

You can redistribute Gateway to your end users after you customize it for the features in your product and for your company's branding.

How to view the terms and conditions for redistribution is described in [Redistributing ISIS End User Applications](#) on page 4.

This chapter includes:

- [Redistributable Gateway Files for Windows](#) on page 26
- [Redistributable Files for Apple Macintosh](#) on page 27
- [About the Branding File](#) on page 27
- [Branding File Format](#) on page 28
- [Branding for Different Languages](#) on page 29
- [Changing Branding](#) on page 30
- [Creating an Alternate Workflow](#) on page 38
- [Creating a Gateway Installer for Windows](#) on page 41

## Redistributable Gateway Files for Windows

When you install the ISIS toolkit, a distributable copy of Gateway is installed in your **My Documents** folder.

You can open the folder containing the distributable copy by doing one of:

- Selecting **Start - PLX Technology - ISIS - Redistributables - Gateway**
- Using Windows Explorer to navigate to **My Documents\PLX Technology\ISIS\Gateway\Vx.y.z** (where x.y.z is the version of ISIS toolkit). Open the 32-bit or 64-bit folder as relevant

Gateway consists of the following:

- Gateway.exe—the main Gateway executable
- DiskFormatter.exe—an executable that formats and partitions hard disks. Requires administrator privileges
- \*.dll—support DLLs used by Gateway
- Flashes.xml—file describing the supported flash devices



If you have modified the contents of Flashes.xml, you must replace the one in this folder with your modified version

- GatewaySupport— folder containing Gateway branding and customization files:
  - An icon file used in the title bar of Gateway windows
  - Graphics files used to brand product, watermark the dialog boxes and similar
  - branding.xml—a file that contain all the branding and customization information, messages to be displayed, information on which graphics files to use where and what features are supported. For more information, see [About the Branding File](#) on page 27
  - branding\_\*.xml—files containing information for other languages. For more information see [Branding for Different Languages](#) on page 29
- DriverInstaller.exe—an executable that installs any device drivers required by Gateway. For more information see [Creating a Gateway Installer for Windows](#) on page 41
- Drivers—folder containing any device drivers installed by DriverInstaller.exe

## Redistributable Files for Apple Macintosh

To create an Apple Macintosh redistributable Gateway package, you must manually copy the **DistributableFiles** folder to your host when installing Gateway (see [Installing the ISIS Firmware Updater or Gateway on an Apple Macintosh host](#) on page 3).

The DistributableFiles folder contains the following files:

- Gateway—the main Gateway executable. This contains the **Flashes.xml** file and **GatewaySupport** folder. These are identical to those contained in an equivalent Windows Gateway redistributable. To make changes to the GatewaySupport folder, Ctrl-click on the file and select **Show Package Contents**. The GatewaySupport folder is in **Contents\Resources**
- RemoteComms filter driver—the device driver used to access the PLX Technology device
- Package.pmdoc—the PackageMaker project used to create the dmg file for your Firmware Updater
- License.rtf—a license file which you must modify to contain your own license. Your license can be displayed when Gateway is installed by the end user

## About the Branding File

The branding file is in XML format and is called **branding.xml**. You specify the following types of settings in the branding file:

- Enabling and disabling product features and application dialog boxes
- Changing the layout and appearance of the user interface
- Specifying the vendor and product IDs of the PLX Technology devices that are recognized by Gateway
- Specifying how each product is presented, including graphics for each one

You can edit branding.xml with any text editor and on many development environments. We recommend using a text editor that highlights XML syntax, such as Notepad++ in Windows.

After making changes we recommend that you validate the basic structure of the XML document before starting Gateway. You can do this in many ways, including opening the document using Internet Explorer.

For more information about the file contents, see [Branding File Format](#) and [Branding for Different Languages](#) on page 29. For information on changing branding.xml, see [Changing Branding](#) on page 30.



Any XML node in the branding file containing the attribute **Mac="false"** is only supported by the Windows version of Gateway. Any XML node containing the attribute **Mac="true"** is only supported by the Apple Macintosh version of Gateway. If the attribute is not specified, it is supported by both versions.

## Branding File Format

The branding file branding.xml contains XML comments that explain the use of each section in the file, as illustrated in the example below.

```
<?xml version="1.0" encoding="utf-8"?>
<Branding xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/
XMLSchema">
  <Appearance> <!-- The general appearance and operation of Gateway --> </Appearance>
  <DeviceSupport> <!-- The devices that are supported, and how they are presented -->
    <SupportedVendorIds> <!-- List of Vendor IDs supported --> </SupportedVendorIds>
    <SupportedSCSIVendorIds_Mac="true"> <!-- List of SCSI Vendor IDs supported --> </SupportedSCSIVendorIds>
    <SupportedDevices> <!-- List of Product IDs -->
      <item> <!-- Describes how a single Product Id is supported -->
        <key></key> <!-- The key contains the Product ID -->
        <value>
          <BrandingDevice> <!-- How the device will be supported -->
            <AutoFormat> <!-- Disk format information --> </AutoFormat>
          </BrandingDevice>
        </value>
      </item>
      <!-- The above item is repeated for each supported device -->
    </SupportedDevices>
  </DeviceSupport>
  <LockUnlock> <!-- Customise the Lock/Unlock tab --> </LockUnlock>
  <Passwords> <!-- Customise the Password Management tab --> </Passwords>
  <Setup> <!-- Customise the Setup and Reset tab -->
    <Wizard> <!-- Customise the Setup Wizard -->
      <Start> <!-- Customise the Wizard Start page --> </Start>
      <Raid> <!-- Customise the Wizard RAID page --> </Raid>
      <Encryption> <!-- Customise the Wizard Encryption page --> </Encryption>
      <Miscellaneous> <!-- Customise the Wizard Miscellaneous page --> </Miscellaneous>
      <Completion> <!-- Customise the Wizard Apply Changes page --> </Completion>
      <Format> <!-- Customise the Wizard Format page --> </Format>
    </Wizard>
  </Setup>
  <VirtualCD> <!-- Customise the Virtual CD tab --> </VirtualCD>
  <Preferences> <!-- Customise the Preferences tab --> </Preferences>
  <Resources> <!-- Specifies all the images, icons and colors used -->
    <ColorValues> <!-- Details on the colors used --> </ColorValues>
    <Fonts> <!-- Details of the fonts used --> </Fonts>
    <IconFiles> <!-- Details on the icon files used --> </IconFiles>
    <ImageFiles> <!-- Details on the image files used --> </ImageFiles>
  </Resources>
  <ErrorMessages> <!-- The main error messages --> </ErrorMessages>
</Branding>
```

For information on how to change the entries in branding.xml, see [Branding for Different Languages](#) on page 29 and [Changing Branding](#) on page 30.

## Branding for Different Languages

The Gateway user interface can support several languages: you create a branding file for each language you want. Gateway automatically displays the language that matches the culture settings of the host.

You can include identifiers for the language, or for the language and country, in the branding file name as follows:

branding\_<language>.xml  
branding\_<language>\_<country>.xml

The *language* identifier is a two to four letter code specified by ISO 639. For more details, see [http://en.wikipedia.org/wiki/ISO\\_639](http://en.wikipedia.org/wiki/ISO_639). The shortest code available for a language is used (e.g. **en** for English).

The *country* identifier is defined by ISO 3166. For more details, see [http://en.wikipedia.org/wiki/ISO\\_3166](http://en.wikipedia.org/wiki/ISO_3166).

Gateway selects the most appropriate branding file for the current host regional settings. Gateway first looks for a branding file that contains both language and country code. If this is not found, Gateway looks for a branding file that contains just the language code. For example, when the Brazilian Portuguese regional settings are in use (language **pt**, country **BR**), Gateway looks for files in the following order:

- 1 A branding file called **branding\_pt\_BR.xml**.
- 2 If this is not present, a branding file called **branding\_pt.xml**.
- 3 If neither of these files is present, Gateway uses the default branding file **branding.xml**.

Branding files for different languages can specify product features and user interface appearance details that are different from those in branding.xml or from other language branding files.

In the branding file, text that must be translated is marked by the following XML comments:

```
<!-- vvvvvvvvvvvvvvvv TEXT BELOW HERE CAN BE TRANSLATED vvvvvvvvvvvvvvv -->  
.  
. .  
  
<!-- ^^^^^^^^^^^^^^^^^ END TRANSLATION ^^^^^^^^^^^^^^^^^ -->
```

Do not translate any text that is not marked by these comments.

When translating the Gateway user interface into other languages, follow these guidelines:

- Before starting any translation, ensure you have completed the customization and branding for your default branding.xml file. This minimizes the amount of rework for each translated language
- When translating text, only translate the displayed text. Do not translate boolean strings (for example, true and false), XML tag names or any attribute text strings in tags
- If you translate the graphics file names, you must provide files with these translated names
- Do not change the resource keys used in the file unless you also translate them in the resource list. Usually there is no need to do so

## Changing Branding

When you change the branding file, you can change features available to the end user, change the appearance of the user interface, and change the text used in the user interface.

You can change any item in the branding file. We recommend you use a text editor such as Notepad++, so that you can clearly see the XML tags.



Do not change XML tag text, the boolean strings **true** or **false** or any attribute text strings in tags. These must remain in English.

You can add, change or remove graphics files used. Avoid changing the key name: if you do change it, ensure you change **all** references to the key in the branding file.

Some options change workflow and configuration of Gateway. For more information, see [Creating an Alternate Workflow](#) on page 38.

### Mandatory changes

For each branding file you create, you must change items marked with a comment that starts with:

<!-- MANDATORY CHANGE:

The following table describes the sections that must be changed.

| Item               | Description   |
|--------------------|---|
| SupportedVendorIds | Must include your company vendor identifier(s) in the format of decimal numbers or a hexadecimal number prefixed by <b>0x</b> .<br>If the accompanying tag is false = USB vendor identifier<br>If the accompanying tag is true = FireWire vendor identifier (only supported as part of a USB 3.0/FireWire combi product)                                  |
| SupportedDevices   | Must include an entry for each product identifier you want Gateway to handle, in the format of decimal numbers or a hexadecimal number prefixed by <b>0x</b> .<br>If the BrandingDevice Is1394 entry is false = USB product<br>If the BrandingDevice Is1394 entry is true = FireWire product (only supported as part of a USB 3.0/FireWire combi product) |
| StartupRegistryKey | You must change this key in the Appearance section to something unique for your company. This prevents solutions from other companies causing problems and prevents more than one instance of your version of Gateway from running  |

For more information about where these are in the branding file, see [Branding File Format](#) on page 28.

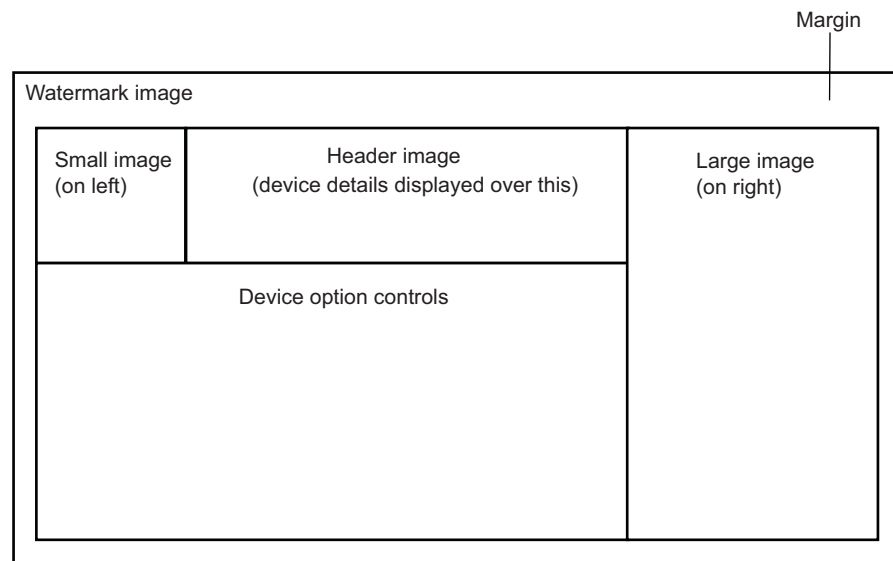
## Changing SCSI vendor information on an Apple Macintosh

As with the Windows version, Gateway only detects devices with the specified USB/FireWire vendor and product IDs. As an additional level of security on an Apple Macintosh, the device must return a specified vendor ID string to a SCSI inquiry command. If you change this inquiry string (either using custom firmware or the Flash Editor), then you must:

- Specify the string in the <SupportedSCSIVendorIds> list in the <DeviceSupport> section
- Carry out additional steps when deploying the package. For details, see [Creating a Gateway Package for Apple Macintosh](#) on page 41

## Changing the user interface appearance

Each window is made up of parts as shown in the following image.



The Appearance section of the branding file contains the settings that control the layout and appearance of Gateway windows. For more information on the sections in the branding file, see [Branding File Format](#) on page 28.

You can change the appearance of windows by:

- [Changing window size](#)
- [Changing window layout](#)
- [Changing the Lock/Unlock window](#)
- [Changing colors](#)
- [Changing watermarks](#)
- [Changing images](#)
- [Changing fonts](#)
- [Changing branding for a specific product](#)

This section also describes [Automatic Disk Formatting](#).

### Changing window size

You can change the size of Gateway windows. For example, you can increase the size if you use large images, or decrease it if you use fewer images. To do so, change the following code, which is in the <Appearance> section of the branding file:

```
<InitialFormSize>
<Width>620</Width>
<Height>460</Height>
</InitialFormSize>
```



## Changing window layout

The following table gives examples of the layout elements you can change.

| Code                                      | Description   |
|---|---|
| <MarginWidth>                             | Windows only.<br>Size of the margin around the edge of the main window.<br>The watermark image is shown in this area                                      |
| <ShowSmallImage><br><SmallImageOnLeft>    | Whether small or large images are shown, and whether the image is shown on the left or right  |
| <ShowSelectionDetailsInHeader>            | Whether the first two rows of text in the device details area shows information on the current device, or the currently selected option                   |
| <OptionButtonAlignment>                   | Windows only.<br>Location of the option buttons in the device control area. These can be aligned along the top or bottom, or stacked on the left or right |
| <ShowHeaderLine><br><ShowHeaderLineUnder> | Whether to show a line across the middle of or under the header   |
| <ShowSingleDeviceDetails>                 | Whether to show details of the attached product in the header if there is only one product attached   |

## Changing the Lock/Unlock window

You can change the size of the Lock/Unlock window, the images displayed in the header to switch between it and the Settings Window, and the text displayed. These are in the <LockUnlock> section of the branding file .The following table gives examples of the lock/unlock elements you can change.

| Code                                | Description  |
|-------------------------------------|--|
| <LockUnlockFormSize>                | Specifies the Lock/Unlock window size  |
| <LockEnterImage><br><LockExitImage> | The images displayed in the header to enter and exit the Lock/Unlock window (the padlock and settings graphics respectively in the default branding) |
| <SeparateLockUnlockPromptShown>     | Whether the word "Settings" is displayed below the settings image  |
| <SeparateLockUnlockStateShown>      | Whether the word "Lock" or "Unlock" is shown beneath the padlock image   |
| <LockUnlockModeTooltip>             | The tooltip displayed when the cursor is over the padlock image  |
| <SettingsModeTooltip>               | The tooltip displayed when the cursor is over the settings image   |

## Changing colors

Colors are specified in the Appearance section in the branding file. Values are given as identifiers that reference colors defined in the Resources section.

You can define different colors for different uses. For example, `<BackgroundColorId>` or `<MarginColorId>`.

Colors are specified in the format AARRGGBB, where:

- A is the alpha value (transparency)
- R is Red
- G is Green
- B is Blue

Values are hexadecimal in the range 00 to FF. To make an item fully transparent, set its alpha value to 00.

## Changing watermarks

You can change:

- The watermark that appears at the back of the window
- The watermark in the Device option control area

The watermark image at the back of the window is only shown when the margin width is greater than 0 or when one of the overlaying colors of a panel is transparent.

For the background of the relevant panel, use a color with an alpha value of 00 (see [Changing colors](#) above).

The following table gives examples of elements for the watermark at the back of the window that you can change; these are in the Resources section of the branding file. The image is stretched or shrunk to fit the area.

| Code                                  | Description                     |
|---------------------------------------|---------------------------------|
| <code>&lt;WatermarkImageId&gt;</code> | The image file to use           |
| <code>&lt;UseWatermark&gt;</code>     | Enable or disable the watermark |

To set a watermark for the Device option controls area, use `<OptionWatermarkImageId>` and `<UseOptionWatermark>`.

## Changing images

Image files are stored in the GatewaySupport folder in the redistributable installation. You specify how to use each image file in the Resources section of the branding file.

The following table shows the default images you can choose to show or not show.

| Code                  | Description   |
|-----------------------|---|
| <DefaultSmallImageId> | Small image—you can place this to the left or right of the window |
| <DefaultLargeImageId> | Header image—appears behind text describing a specific product    |
| <DefaultHeaderId>     | Large image—you can place this to the left or right of the window |

The default images are overridden if you specify different images for each product.

You may need to adjust the size of the window to show your images correctly. For instructions, see [Changing window size](#) on page 32.

## Changing fonts

You can control the fonts used by text in the Gateway user interface using settings in the Fonts section of the Resources section of the branding file. You can set different fonts and sizes for Windows and Apple Macintosh. For each font style, you can specify the following parameters:

| Code    | Description   |
|---------|---|
| WinName | The name of the font to be used in Windows (e.g. Arial)   |
| WinSize | The point size of the font as a floating point number in Windows (e.g. "8.3")                   |
| MacName | The name of the font to be used on an <b>Apple Macintosh</b> (e.g. Arial)                       |
| MacSize | The point size of the font as a floating point number on an <b>Apple Macintosh</b> (e.g. "8.3") |
| Bold    | Whether the font is emboldened (true/false)   |
| Italic  | Whether the font is italicized (true/false)   |

The Appearance section specifies which font style is used for specific text elements by referencing its tag name. For example, the text used for any warning label is specified in Appearance by:

<WarningFontId>warningFont</WarningFontId>

This font style is defined in the Font Resources section as:

```
<item>
  <key>
    <string>warningFont</string>
  </key>
  <value>
    <Font>
      <WinName Mac = "False">Arial</WinName>
      <WinSize Mac = "False">8.3</WinSize>
      <MacName Mac = "True">Arial</MacName>
      <MacSize Mac = "True">10.8</MacSize>
      <Bold>false</Bold>
      <Italic>true</Italic>
    </Font>
  </value>
</item>
```

### Changing branding for a specific product

Any branding you specify for a product (using the Branding Device section of the branding file) overrides other branding specified elsewhere in the branding file (for example, in the Appearance section). To locate the Branding Device section, see [Branding File Format](#) on page 28).

The following table describes product branding settings.

| Code   | Description   |
|--|---|
| <BrandingDevice><br><Is1394>>false</Is1394>  | False = product is attached using USB<br>True = product is attached using FireWire  |
| <AllowLockUnlockControl>>false</AllowLockUnlockControl><br><AllowPasswordControl>>false</AllowPasswordControl><br><AllowSetupControl>true</AllowSetupControl><br><AllowVirtualCdControl>true</AllowVirtualCdControl> | Enables and disables features available for the product.<br>If you enable a feature not supported by the product, fields for that feature are still not displayed |
| <AllowEncryptionControl>>false</AllowEncryptionControl><br><AllowRaidControl>>false</AllowRaidControl><br><AllowMiscellaneousControl>true</AllowMiscellaneousControl>  | Enables and disables pages in the drive setup wizard  |
| <ShortName>OXU3100</ShortName><br><PrimaryDetails>USB3 External Drive</PrimaryDetails><br><SecondaryDetails>PLX Technology</SecondaryDetails><br><DeviceDetails>PLX Technology OXU3100</DeviceDetails>               | Text shown for a product  |
| <SmallImageId>smallImage3100</SmallImageId><br><LargeImageId>largeImage</LargeImageId><br><HeaderImageId>headerImage</HeaderImageId>   | Images shown for a product.<br>Any images specified here override images specified in the Appearance section (see <a href="#">Changing images</a> on page 34)     |
| <AutoFormat><br>...<br></AutoFormat><br></BrandingDevice>  | Controls whether any disk is automatically formatted, and the parameters of this format. For more details, see <a href="#">Automatic Disk Formatting</a>          |

## Automatic Disk Formatting

In the DeviceBranding section of the branding file, there is an Autoformat subsection for each device. This specifies whether any disk is automatically reformatted after a reset or after configuration changes that lose all the disk content. Note that automatic disk formatting is not supported for RAID devices configured with independent disks (JBOD).

The following table describes the settings in the Autoformat section.

| Code  | Description   |
|---|---|
| <SupportDeviceFormat>true</SupportDeviceFormat> | Whether auto-formatting is supported. If not, Windows Disk Management is displayed as an option on the drive setup wizard Format page   |
| <QuickFormat>true</QuickFormat>                 | Whether a quick format is performed   |
| <FileSystem>NTFS</FileSystem>                   | Windows only.<br>The file system to use on Windows.<br>This can be NTFS, FAT16 or FAT32   |
| <PartitionType>primary</PartitionType>          | Windows only.<br>The disk partition type to create on Windows.<br>For details on possible values, see the Microsoft Windows documentation about the diskpart command line utility   |
| <DisableGPT>false</DisableGPT>                  | Windows only.<br>False = for Windows Vista or later, with a disk greater than 2.2TB, GPT partitioning scheme is used<br>True = for Windows Vista or later, with any size disk, MBR partitioning is used, which limits the disk capacity to 2.2TB<br>For Windows XP this entry is ignored. To use disks that are greater than 2.2TB, you must use 4K sectors |
| <MacFileSystem>jhfs+</MacFileSystem>            | Apple Macintosh only.<br>The file system to use on an Apple Macintosh. This can be FAT16, FAT32, hfs+, hfsx, jhfsx or jhfs+.  |
| <MacPartitionType>APM</MacPartitionType>        | Apple Macintosh only.<br>If APM, then APM partitions are used on an Apple Macintosh. Otherwise MBR is used  |
| <VolumeName>USB3_HDD</VolumeName>               | The name of the volume. The volume name may contain spaces. However, if you are formatting the volume on Windows XP, spaces are replaced by _ (underscore)  |

## Creating an Alternate Workflow

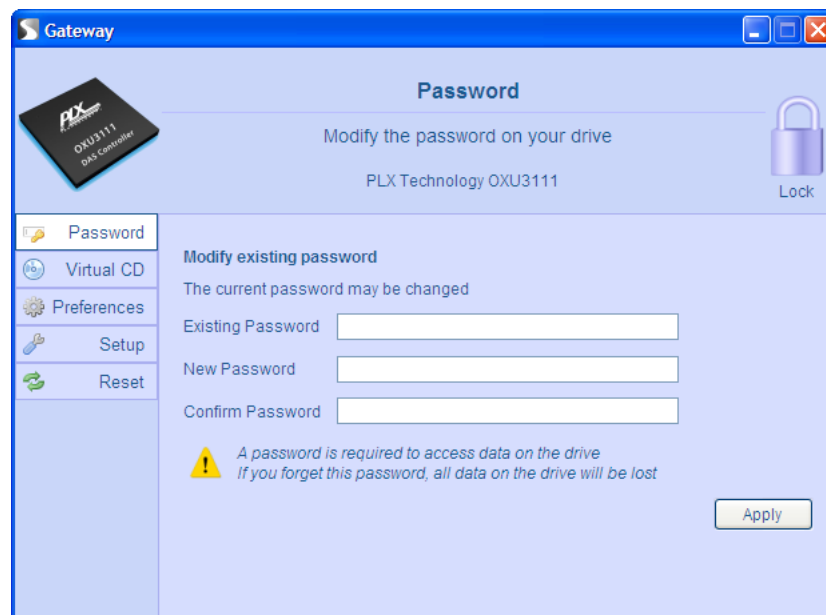
Certain combinations of options in the branding file may trigger alternate workflows and configurations of Gateway. This section describes some examples of these.

### Single password drive locking

For encrypted devices that support password-controlled drive locking, the device supports up to 10 passwords. You can restrict your end user to only define a single password. You can do so by setting the following:

| Section        | Code                    | Set to |
|----------------|-------------------------|--------|
| DeviceBranding | <Allow PasswordControl> | true   |
| Passwords      | <ShowAddPassword>       | false  |
|                | <ShowDeletePassword>    | false  |
|                | <ShowModifyPassword>    | true   |

You must also modify the text displayed to clearly describe the single password operation. This retains a separate password tab just allowing the single password to be modified, as shown below:

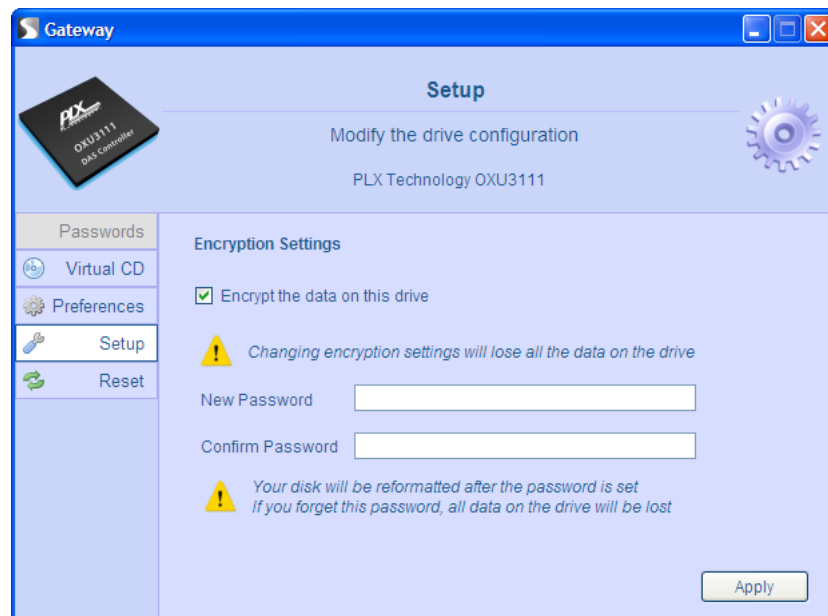


## Single setup window for encryption and password setup

You can set the drive setup wizard to have a single setup window with only encryption enabling and password creation. To do so, set the following:

| Code                        | Set to |
|-----------------------------|--------|
| <AllowRaidControl >         | false  |
| <AllowMiscellaneousControl> | false  |
| <AllowEncryptionControl >   | true   |
| <ShowEncryptionMode>        | false  |
| <ShowEncryptionKeyStrength> | false  |
| <ShowEnableEncryption>      | true   |
| <ShowPasswordInitialise>    | true   |

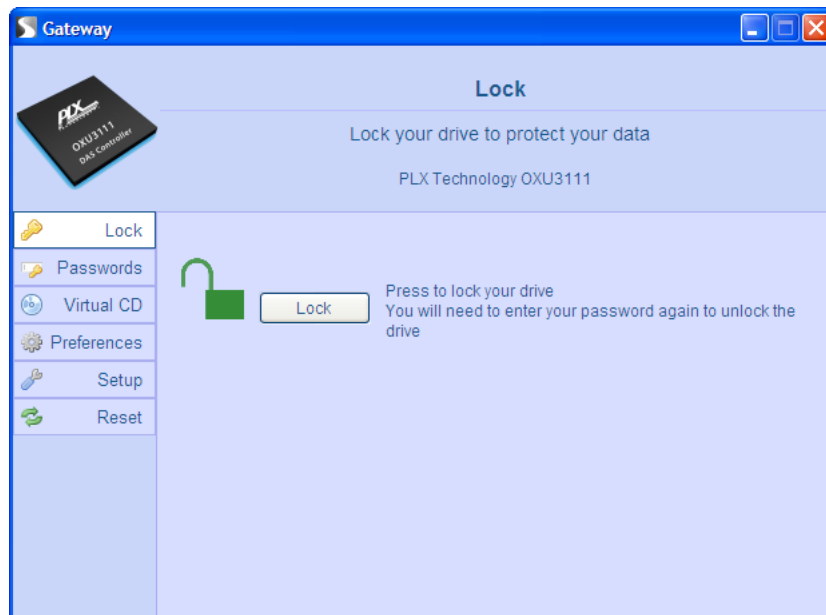
The setup window looks similar to the following image.



Note that the password fields are only shown when you check the **Encrypt the data on this drive** option.

## Integrating lock/unlock options in a single Gateway main window

By default, Gateway shows the lock/unlock options in a separate window. You can choose to display all Gateway options as tabs in a single main window. To do so, set the <SeparateLockUnlock> element in the <LockUnlock> section of the branding file to false. In this configuration, the Lock/Unlock option appears as a tab on the main window, and the Settings/Padlock icon in the header is no longer shown.





## Creating a Gateway Installer for Windows

We strongly recommend that the Gateway version you distribute to end users includes an installer branded to your company. We recommend you build the installer using an installer creation utility such as InstallShield or WiX.

Your installer must install the contents of the redistributable Gateway 32-bit or 64-bit folder into a folder in **Program Files**. To enable your end users to start Gateway easily, you must create a link to **Gateway.exe** in the Windows Start menu.

You can use the same branded and customized version of the GatewaySupport folder for both your 32-bit and 64-bit installations.

The redistributable Gateway folder contains the executable **DriverInstaller.exe**. This must be run from your installer. Installing drivers requires full administrator rights, which Gateway does not have, so this must be performed separately at installation time

To ensure that both Gateway drivers and application can be installed, we strongly recommend that:

- Your installer requires administrator rights to run
- Your installer automatically runs the DriverInstaller.exe at the end of the installation, once Gateway is installed
- You set DriverInstaller.exe to run asynchronously and to not wait for any exit code. This ensures that DriverInstaller.exe runs to completion once your installer finishes

If you intend to use the WiX installer toolkit to create your installer (free from <http://wix.sourceforge.net>), we can provide a sample installer project on request, from which you can start your development.

## Creating a Gateway Package for Apple Macintosh

When redistributing Gateway for the Apple Macintosh, you must create a disk image (dmg), to ensure the required device drivers are installed. We provide a PackageMaker project from which you create your customized dmg file. The PackageMaker file, called **Package.pmdoc**, is in the root of the RedistributableFiles folder you copied to your host when you installed the ISIS toolkit.

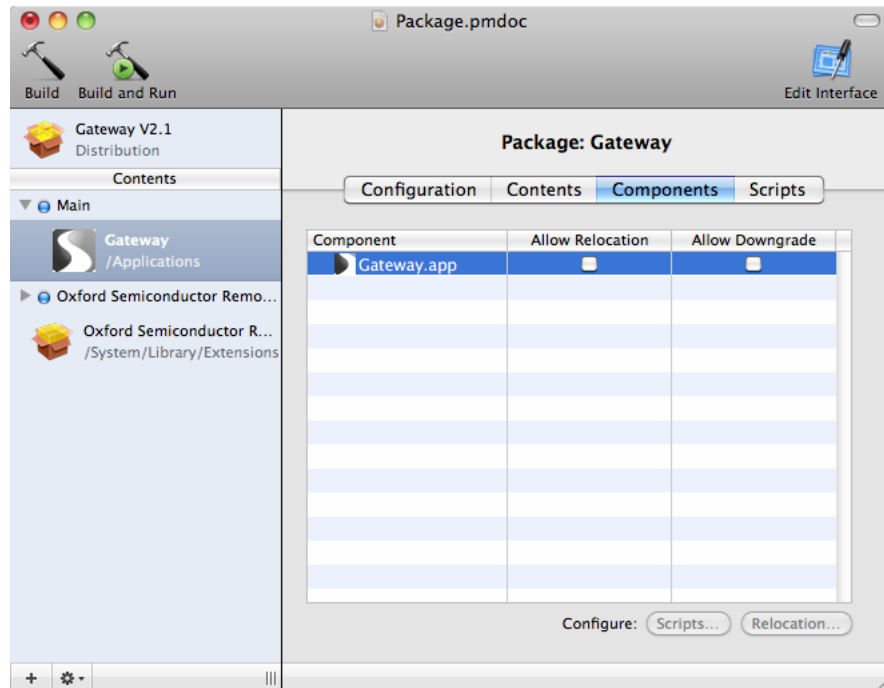


To open this file, you must have Xcode 3.2 installed. If you do not have Xcode installed, this appears as a normal folder. In this case, download and install Xcode 3.2 before continuing. After installing Xcode, you must initialize PackageMaker by running PackageMaker once from the Xcode Utilities folder. You can then open the folder by double-clicking.

Make the changes you want to the Gateway executable package, then create your own dmg file. To do so:

- 1 In the RedistributableFiles folder, double-click Package.pmdoc. The message **Resources Found** is shown.
- 2 Select **Do Not Use**.
- 3 Expand Gateway in the left hand column and select the Gateway application.

- 4 In the Components tab, ensure **Allow Relocation** is unchecked. The generated package does not work if you leave this option checked.

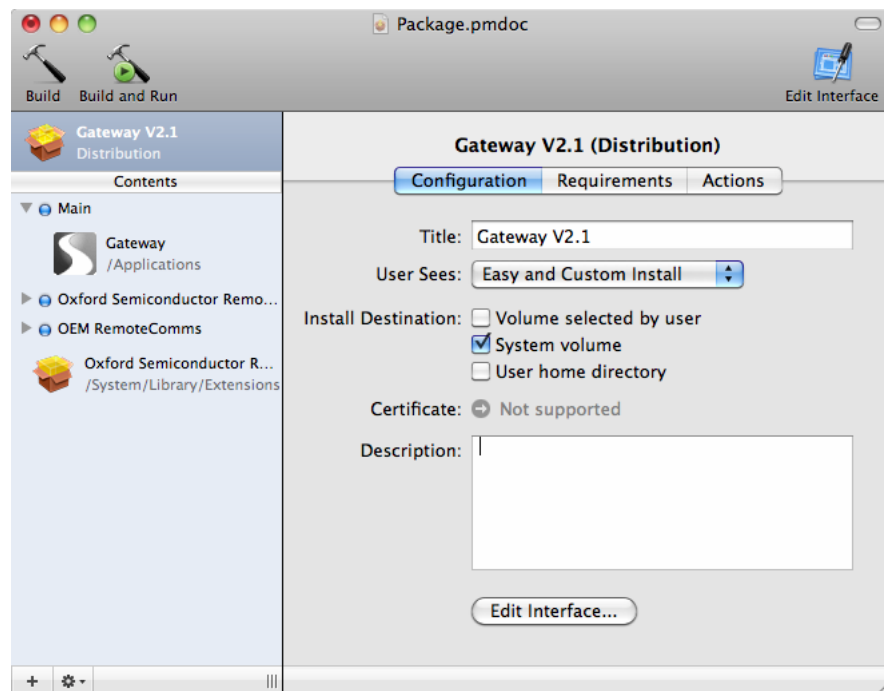


- 5 Make any other changes you require to the package, such as version number, displaying a readme file, or further company-specific branding. For more details, see the PackageMaker documentation.
- 6 Click **Build**. Select the location to save the dmg file in and click **Save**.

If you change the vendor ID string returned for a SCSI inquiry command from the default value of "OEM ", you must:

- Specify this value in the branding file (see [Changing SCSI vendor information on an Apple Macintosh](#) on page 31)
- Create a custom RemoteComms driver layer and add it to this package. For details of creating the driver layer, see Chapter 7 [Creating a RemoteComms Driver Layer for Apple Macintosh](#).

To add your driver layer to the disk image for your Gateway package, click the **+** button at the bottom left of PackageManager and select your driver layer. This example shows a driver layer package called OEM RemoteComms.



This page is intentionally blank

## Using the Firmware Updater

The Firmware Updater enables your end users to update the firmware for your products.

You can redistribute the Firmware Updater to your end users after you customize it to match your company branding and firmware details for your products. This chapter describes the Firmware Updater as supplied. For instructions on customizing, see Chapter 6 [Customizing and Deploying the Firmware Updater](#).

The Firmware Updater leaves device configuration information unchanged. You use the Firmware Updater to:

- Update firmware flash sectors
- For ROM-based products, to deploy a firmware patch file

The Firmware Updater appears to the user to operate in the same way, whether you are updating firmware in flash or patching ROM-based firmware.

This chapter includes:

- [Firmware Updater Features](#) on page 45
- [Starting the Firmware Updater and Updating Firmware in Windows](#) on page 46
- [Closing the Firmware Updater](#) on page 47
- [Resuming an Interrupted Update](#) on page 48
- [Using the Firmware Updater on Apple Macintosh](#) on page 48

To run the Firmware Updater on your host PC, you must have administrator rights on the PC. You can only update one product at a time.

### Firmware Updater Features

You can:

- Specify the firmware update(s) to use for each of your products
- Specify the version, or range of versions, of existing firmware that an update applies to
- Revert to the original firmware if the update process fails. A copy of the existing firmware content is made before making any changes
- Automatically present a user interface translated to the current operating system language, where supported
- Present custom graphics for each supported product

The supplied Firmware Updater is configured to update a PLX Technology OXU310x or OXU311x device with a sample version of software, for demonstration purposes only. This may not be the latest version of firmware for the device in your evaluation kit or in the ISIS toolkit.

Before you use the sample firmware update, ensure you know how to update your PLX Technology OXU310x or OXU311x device with the latest version of firmware. For instructions on how to do this, see Chapter 6 [Customizing and Deploying the Firmware Updater](#).

## Starting the Firmware Updater and Updating Firmware in Windows

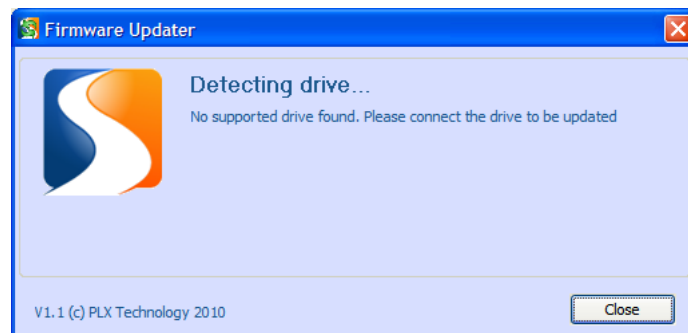
You must have administrator rights on your host PC to run the Firmware Updater.

- 1 When you install the ISIS toolkit, only a redistributable version of the Firmware Updater is installed. You can start this by doing one of the following:
  - ☐ Select **Start - PLX Technology - ISIS - Redistributables - Firmware Updater**
  - ☐ Use Windows Explorer to navigate to **My Documents\PLX Technology\ISIS\FirmwareUpdater\Vx.y.z** (where x.y.z is the version of ISIS toolkit). Open the 32-bit folder and double-click **FirmwareUpdater.exe**

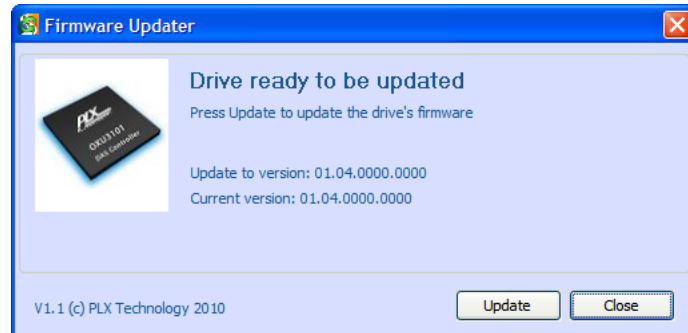


The 32-bit Firmware Updater supports operation on both 32- and 64-bit Windows.

- 2 If you have installed Gateway, all necessary drivers are already installed. Otherwise, the Firmware Updater automatically installs the drivers when you start it.
- 3 If no product is attached, the Detecting Drive window is shown.



If a product is attached, or you attach one, the Drive ready window is shown.



This shows an image of the PLX Technology device, the current version of firmware and the update version. It also shows the version string contained in the branding file, in the bottom left of the window. (You can customize the image to show an image of your product; see Chapter 6 [Customizing and Deploying the Firmware Updater](#).)

- 4 To update the firmware, click **Update**. Progress information is shown in the window, and an indication when the update is complete.
- 5 The Firmware Updater restarts the product and reads the updated firmware to verify it. The firmware version and a completion message are shown.

If an error occurs during the update process, the Firmware Updater retries the update. If this fails, the Firmware Updater tries to restore the original firmware and configuration information.



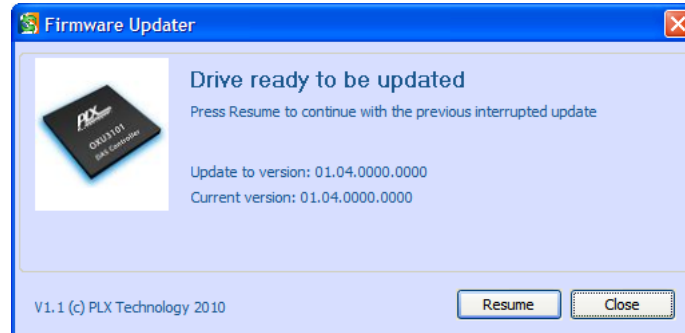
If you modify the vendor name returned by your device to a SCSI inquiry command, the Firmware Updater cannot detect the device. This is because the Firmware Updater is configured to only recognize a device from a specific vendor. For instructions on how to make the Firmware Updater detect your modified device, see [Branding File Format](#) on page 54.

## Closing the Firmware Updater

To close the Firmware Updater click **X** (Windows Close button) in the top right of the window. You are asked if you want to complete any update in progress before closing.

## Resuming an Interrupted Update

You can restart an update that was interrupted, for example by a power failure. To resume an update, restart the Firmware Updater (see [Starting the Firmware Updater and Updating Firmware in Windows](#) on page 46). The Drive ready window is shown, with the **Resume** button enabled.



Click **Resume**. The same progress messages are shown as described in [Starting the Firmware Updater and Updating Firmware in Windows](#) on page 46.

## Using the Firmware Updater on Apple Macintosh

The operation of the Firmware Updater on an Apple Macintosh is identical to Windows. After installing the Firmware Updater, you open it from the Macintosh Utilities folder.





## Customizing and Deploying the Firmware Updater

You can redistribute the Firmware Updater to your end users after you customize it for the features in your product and for your company's branding.

How to view the terms and conditions for redistribution is described in [Redistributing ISIS End User Applications](#) on page 4.

This chapter includes:

- [Windows Redistributable Files](#) on page 50
- [Apple Macintosh Redistributable Files](#) on page 51
- [Specifying Products and Firmware Images](#) on page 51
- [Changing Branding](#) on page 53
- [Branding File Format](#) on page 54
- [Branding for Different Languages](#) on page 58
- [Creating a Firmware Updater Package for Windows](#) on page 59
- [Creating a Firmware Updater Package for Apple Macintosh](#) on page 59

## Windows Redistributable Files

When you install the ISIS toolkit on a Windows host, only a redistributable version of the Firmware Updater is installed. You can open the folder containing the distributable copy by doing one of:

- Selecting **Start - PLX Technology - ISIS - Redistributables - Firmware Updater**
- Using Windows Explorer to navigate to **My Documents\PLX Technology\ISIS\FirmwareUpdater\Vx.y.z** (where x.y.z is the version of ISIS toolkit). Open the 32-bit folder



The 32-bit Firmware Updater supports operation on both 32- and 64-bit Windows.

The Firmware Updater consists of:

- FirmwareUpdater.exe—the main Firmware Updater executable
- \*.dll—support DLLs used by the Firmware Updater
- Flashes.xml—file describing the supported flash devices



If you have modified the contents of Flashes.xml, you must replace the one in this folder with your modified version.

- FirmwareUpdaterSupport—folder containing the Firmware Updater branding and customization files, including:
  - Firmware—folder containing the firmware files and information on which products are supported. For more details, see [Specifying Products and Firmware Images](#) on page 51
  - Branding—folder containing the branding of the application. This includes text, images and different language information. For more details, see [Changing Branding](#) on page 53 and [Branding for Different Languages](#) on page 58
- DriverInstaller.exe—executable that installs the device drivers required by the Firmware Updater. This is automatically run by the Firmware Updater if needed
- Drivers—folder containing the device drivers that may be installed by DriverInstaller.exe

## Apple Macintosh Redistributable Files

To create an Apple Macintosh redistributable Firmware Updater package, you must manually copy the **DistributableFiles** folder to your host when installing the Firmware Updater (see [Installing the ISIS Firmware Updater or Gateway on an Apple Macintosh host](#) on page 3).

The DistributableFiles folder contains the following files:

- FirmwareUpdater—the main Firmware Updater executable. This contains the **Flashes.xml** file and **FirmwareUpdaterSupport** folder. These are identical to those contained in an equivalent Windows Firmware Updater. To make changes to the FirmwareUpdaterSupport folder, Ctrl-click on the file and select **Show Package Contents**. The FirmwareUpdaterSupport folder is in **Contents\Resources**
- RemoteComms Driver—the device driver used to access the PLX Technology device
- Package.pmdoc—the PackageMaker project used to create the dmg file for your Firmware Updater
- License.rtf—a license file which you must modify to contain your own license. Your license can be displayed when the Firmware Updater is installed by the end user

## Specifying Products and Firmware Images

You use files in the FirmwareUpdaterSupport\Firmware folder to specify:

- Products to update
- Version of firmware, or range of versions of firmware to update
- Firmware or patch files to use. See [Specifying firmware or patch files](#)

These details are contained in the file **UpdateInfo.xml**. For details of what you can change, see [Changing UpdateInfo.xml](#) on page 52.

### Specifying firmware or patch files

The UpdateInfo file supplied supports all PLX Technology OXU310x and OXU311x devices. It updates the firmware version using one of the following:

- For a flash-based product, the firmware image file **FirmwareUpdaterSupport\U31xx\_Firmware.pfw**, where x is replaced with 0, 1 or 2 according to the device name
- For a ROM-based product, the patch file **FirmwareUpdateSupport\U311x\_Patch.pfp**, where x is replaced with 0 or 1 according to the device name

Ensure you place in FirmwareUpdaterSupport the firmware image files you want to use in your updates.



You can use the Firmware Updater to upgrade firmware during your development process. For example, if you do not have the Flash Editor installed, use the Firmware Updater instead. To do so, replace the relevant U31xx\_Firmware.pfw or U311x\_Patch.pfp file in FirmwareUpdaterSupport with a file of the same name. To run the Firmware Updater, see Chapter 5 [Using the Firmware Updater](#).

## Changing UpdateInfo.xml

You can edit UpdateInfo.xml with any text editor and on many development environments. We recommend using a text editor that highlights XML syntax, such as Notepad++ in Windows.

After making changes we recommend that you validate the basic structure of the XML document before starting the Firmware Updater. You can do this in many ways, including opening the document using Internet Explorer.

Firmware update details are specified in:

- For a flash-based device, the tag <FirmwareFileName>
- For a ROM-based device, the tag <PatchFileName>

The following table shows examples of the sections in UpdateInfo.xml.

| Section  | Description  |
|--|--|
| <UpdateInfo xmlns="http://www.plxtech.com/ISIS/Update">  | Do not change  |
| <VID id="0x0525">  | Section for hexadecimal USB vendor identifier of 0525  |
| <PID id="0x3110">  | Section for a product with the hexadecimal USB product identifier of 3110 (ROM-based device)   |
| <UpdateBundle>   | Section to describe one update for this product  |
| <Type>Range</Type>   | This value must be <b>Range</b>  |
| <TargetVersionLower>0.0.0.0</TargetVersionLower><br><TargetVersionUpper>FF.FF.FFFF.FFFF</TargetVersionUpper><br><PatchFileName>U3110_Patch.pfp</PatchFileName> | This section defines the range of ROM firmware versions the update patch applies to. If the ROM firmware version is between <b>TargetVersionLower</b> and <b>TargetVersionUpper</b> (inclusive), the firmware is upgraded using <b>PatchFileName</b> .<br>Firmware version must be between 0.0.0.0 and FF.FF.FFFF.FFFF. This example updates any version of firmware to the firmware in the file U3110_Patch.pfp |
| </UpdateBundle>  | End of section describing this update for this product   |
| </PID>   | End of section for this product  |
| <PID id="0x3101">  | Section for a product with the hexadecimal USB product identifier of 3101  |
| <UpdateBundle>   | Section to describe one update for this product  |
| <Type>Range</Type>   | This value must be <b>Range</b>  |

| Section  | Description   |
|--|---|
| <pre> &lt;TargetVersionLower&gt;0.0.0.0&lt;/TargetVersionLower&gt; &lt;TargetVersionUpper&gt;1.0.0.0&lt;/TargetVersionUpper&gt; &lt;FirmwareFileName&gt;U3101_Firmware1.pfw&lt;/ FirmwareFileName&gt; &lt;/UpdateBundle&gt; &lt;UpdateBundle&gt; &lt;Type&gt;Range&lt;/Type&gt; &lt;TargetVersionLower&gt;1.0.0.1&lt;/TargetVersionLower&gt; &lt;TargetVersionUpper&gt;FF.FF.FFFF.FFFF&lt;/ TargetVersionUpper&gt; &lt;FirmwareFileName&gt;U3101_Firmware2.pfw &lt;/FirmwareFileName&gt;  &lt;/UpdateBundle&gt; </pre> | <p>Different firmware files are being used to upgrade different firmware versions. In this example:</p> <ul style="list-style-type: none"> <li>■ U3101_Firmware1.pfw is used if the product firmware is between 0.0.0.0 and 1.0.0.0 inclusive</li> <li>■ U3101_Firmware2.pfw is used for any other version of product firmware</li> </ul> <p>Note that if the second <b>UpdateBundle</b> section is omitted, the update only takes place if the original firmware is within the range 0.0.0.0 to 1.0.0.0; no update occurs for later versions</p> |
| ...  | Further update ranges for this product can be added here  |
| </PID>   | End of section for this product   |
| <pre> &lt;PID&gt; ... &lt;/PID&gt; ... </pre>  | Further products for this USB vendor identifier   |
| </VID>   | End of section for this USB vendor identifier   |
| <pre> &lt;VID id="0x0928"&gt; ... &lt;/VID&gt; </pre>  | A different USB vendor identifier, with further product entries   |
| </UpdateInfo>  | End of the file   |

## Changing Branding

The files controlling Firmware Updater branding are in FirmwareUpdaterSupport\Branding. You can change:

- Layout and appearance of the window
- Graphics and text displayed
- Languages supported
- The vendor ID that must be returned by the device in response to a SCSI inquiry, to ensure the device is recognized by the Firmware Updater

The folder contains the following files:

- Branding.xml—contains the text to be displayed, and layout and appearance of the window. For more information see [Branding File Format](#) on page 54
- Branding\_\*.xml—files containing information for other languages. For more information see [Branding for Different Languages](#) on page 58
- Product.ico—icon displayed in the window title bar
- DefaultLogo.bmp—graphic displayed in the window when no product is present

- `image_xxxx_yyyy.bmp`—image to display when working with a product of USB vendor identifier `xxxx` and product identifier `yyyy` (in hexadecimal format). If not present, `DefaultLogo.bmp` is used instead

The required size of the bitmaps is dependent on the size of the image specified in the `branding.xml` file. For more details, see [Branding File Format](#).

## Branding File Format

You use the branding file to specify the text, appearance, size and position of every aspect of the user interface. The following table describes the contents of the file and the use of each specific element.

When changing the branding file we recommend you use a text editor such as Notepad++, so that you can clearly see the XML tags.

| Section  | Description  |
|--|--|
| <code>&lt;Branding xmlns="http://www.plxtech.com/ISIS/Updater"&gt;</code>  | Do not change  |
| <code>&lt;FileStore&gt;"PlxTech\ISIS\FirmwareUpdater"&lt;/FileStore&gt;</code>   | The Firmware Updater stores temporary files during its operation, in the Windows Application Data folder for the current user (such as <code>C:\Documents and Settings\&lt;user_name&gt;\Application Data</code> ). Change the <b>FileStore</b> value to specify the name of the folder in which to store this data  |
| <code>&lt;ScsiVid&gt;"OEM "&lt;/ScsiVid&gt;</code>   | The Firmware Updater only detects devices with the specified USB vendor and product IDs. As an additional level of security, the device must return a specified vendor ID string to a SCSI inquiry command. If you change this inquiry string (either using custom firmware or the Flash Editor), then you must: <ul style="list-style-type: none"> <li>■ Specify the string in this section of the branding file</li> <li>■ Carry out additional steps when deploying the package on an Apple Macintosh. For details, see <a href="#">Creating a Firmware Updater Package for Apple Macintosh</a> on page 59</li> </ul> |
| <code>&lt;Messages&gt;</code><br><code>&lt;Message id="0x00"&gt;</code><br><code>&lt;!--There is no firmware found to update this device--&gt;</code><br><code>&lt;Text&gt;"Device firmware is already up to date"&lt;/Text&gt;</code><br><code>&lt;Caption&gt;"Update Information"&lt;/Caption&gt;</code><br><code>&lt;Type&gt;0x00000040&lt;/Type&gt;</code><br><code>&lt;/Message&gt;</code><br><code>&lt;Message id="0x01"&gt;</code><br><code>...</code><br><code>&lt;/Message&gt;</code><br><code>...</code><br><code>&lt;/Messages&gt;</code> | <p>Message boxes to display, for example for error messages. These are referenced by <b>Message id</b> in the rest of the branding file.</p> <p>Include a comment to describe the message.</p> <p>The <b>Caption</b> appears in the title bar of the message box, and the <b>Text</b> appears in the body.</p> <p>For the meaning of values in <b>Type</b>, see <a href="#">Message box types</a> on page 57.</p> <p><b>Accept</b> and <b>Decline</b> tags are unused</p>  |
| <code>&lt;TextList&gt;</code><br><code>&lt;!--Header Texts--&gt;</code><br><code>&lt;Caption id="0x00"&gt;"Detecting device"&lt;/Caption&gt;</code><br><code>&lt;Caption id="0x01"&gt;"Update initialised"&lt;/Caption&gt;</code><br><code>...</code><br><code>&lt;/TextList&gt;</code>  | Text messages to display during the update process. Each has a <b>Caption id</b> and associated text   |

| Section   | Description  |
|---|--|
| <pre> &lt;Colours&gt; &lt;Colour id="0x00"&gt; &lt;Red&gt;215&lt;/Red&gt; &lt;Green&gt;222&lt;/Green&gt; &lt;Blue&gt;255&lt;/Blue&gt; &lt;/Colour&gt; &lt;Colour id="0x01"&gt; ... &lt;/Colour&gt; ... &lt;/Colours&gt; </pre>  | <p>Colors to use; these are referenced in the rest of the branding file. Each has a <b>Colour id</b>. Red, Green and Blue components are in the range 0 to 255</p>   |
| <pre> &lt;Fonts&gt; </pre>  | <p>Font styles to use; these are referenced in the rest of the branding file. Each has a <b>Font id</b>, a <b>Colour id</b>, <b>Size</b> specified in points and <b>Weight</b> in the range 0-1000. As a guide, Windows defines the following weights for font styles:</p> <ul style="list-style-type: none"> <li>■ Thin: 100</li> <li>■ Extra Light: 200</li> <li>■ Light: 300</li> <li>■ Normal: 400</li> <li>■ Medium: 500</li> <li>■ Semi Bold: 600</li> <li>■ Bold: 700</li> <li>■ Extra Bold: 800</li> <li>■ Heavy: 900</li> </ul> |
| <pre> &lt;Font id="0x00"&gt; &lt;Colour&gt;1&lt;/Colour&gt; &lt;Size&gt;18&lt;/Size&gt; &lt;Weight&gt;900&lt;/Weight&gt; &lt;/Font&gt; </pre>   | Font 0 is used in the header   |
| <pre> &lt;Font id="0x01"&gt; &lt;Colour&gt;2&lt;/Colour&gt; &lt;Size&gt;20&lt;/Size&gt; &lt;Weight&gt;990&lt;/Weight&gt; &lt;/Font&gt; &lt;/Fonts&gt; </pre>  | Font 1 is used in the body of a window   |
| <pre> &lt;Frame&gt; &lt;Colour&gt;0&lt;/Colour&gt; &lt;Text&gt;"Firmware Updater"&lt;/Text&gt; &lt;Position&gt; &lt;Left&gt;500&lt;/Left&gt; &lt;Top&gt;100&lt;/Top&gt; &lt;Width&gt;515&lt;/Width&gt; &lt;Height&gt;250&lt;/Height&gt; &lt;/Position&gt; &lt;/Frame&gt; </pre> | Defines the size and position of the main Firmware Updater window, the background color and text displayed in the title bar  |

| Section   | Description  |
|---|--|
| <pre> &lt;TextBoxes&gt; &lt;TextBox id="0"&gt; &lt;Font&gt;1&lt;/Font&gt; &lt;Position&gt; &lt;Left&gt;130&lt;/Left&gt; &lt;Top&gt;18&lt;/Top&gt; &lt;Width&gt;370&lt;/Width&gt; &lt;Height&gt;26&lt;/Height&gt; &lt;/Position&gt; &lt;Colour&gt;0x00&lt;/Colour&gt; &lt;Border&gt;0&lt;/Border&gt; &lt;ModalFrame&gt;0&lt;/ModalFrame&gt; &lt;Visible&gt;1&lt;/Visible&gt; &lt;/TextBox&gt; &lt;TextBox id="1"&gt; ... &lt;/TextBox&gt; ... &lt;/TextBoxes&gt; </pre>                      | <p>Information is displayed in text boxes in a window. There are comments in the supplied branding file that explain the use of each text box.</p> <p>For each text box, you can specify:</p> <ul style="list-style-type: none"> <li>■ Size and position</li> <li>■ Border width</li> <li>■ Color</li> <li>■ Font style</li> </ul> <p>To put an embossed frame around the text box, set the <b>ModalFrame</b> value to 1.</p> <p>To prevent a specific text box from being displayed, set <b>Visible</b> to 0.</p> |
| <pre> &lt;Buttons&gt; &lt;Button id="0x00"&gt; &lt;Colour&gt;3&lt;/Colour&gt; &lt;Font&gt;0&lt;/Font&gt; &lt;TextList&gt; &lt;Caption id="0"&gt;"Update"&lt;/Caption&gt; &lt;Caption id="1"&gt;"Resume"&lt;/Caption&gt; &lt;/TextList&gt; &lt;Position&gt; &lt;Left&gt;330&lt;/Left&gt; &lt;Top&gt;184&lt;/Top&gt; &lt;Width&gt;80&lt;/Width&gt; &lt;Height&gt;24&lt;/Height&gt; &lt;/Position&gt; &lt;/Button&gt; &lt;Button id="0x01"&gt; ... &lt;/Button&gt; ... &lt;/Buttons&gt; </pre> | <p>Button controls that support user interaction. There are comments in the supplied branding file that explain the use of each button.</p> <p>For each button, you can specify:</p> <ul style="list-style-type: none"> <li>■ Size and position</li> <li>■ Color</li> <li>■ Font style</li> <li>■ Text on the button</li> <li>■ Alternate text for buttons that change their text label depending on the state of the update process</li> </ul>  |
| <pre> &lt;ProgressBar id="0"&gt; &lt;Position&gt; &lt;Left&gt;15&lt;/Left&gt; &lt;Top&gt;138&lt;/Top&gt; &lt;Width&gt;479&lt;/Width&gt; &lt;Height&gt;25&lt;/Height&gt; &lt;/Position&gt; &lt;Smooth&gt;0&lt;/Smooth&gt; &lt;/ProgressBar&gt; </pre>  | <p>Progress bar to display during the update process.</p> <p>You can specify</p> <ul style="list-style-type: none"> <li>■ Size</li> <li>■ Position</li> <li>■ Visual style: for the bar to be updated in discrete blocks, set <b>Smooth</b> to 0; for the bar to be updated smoothly, set <b>Smooth</b> to 1</li> </ul>  |



| Section  | Description   |
|--|---|
| <pre> &lt;Group&gt; &lt;Position&gt; &lt;Left&gt;3&lt;/Left&gt; &lt;Top&gt;0&lt;/Top&gt; &lt;Width&gt;503&lt;/Width&gt; &lt;Height&gt;172&lt;/Height&gt; &lt;/Position&gt; &lt;/Group&gt; </pre>   | Border to visually group and delineate user interface controls. You can specify the size and position of the group border   |
| <pre> &lt;Image&gt; &lt;Position&gt; &lt;Left&gt;15&lt;/Left&gt; &lt;Top&gt;20&lt;/Top&gt; &lt;Width&gt;100&lt;/Width&gt; &lt;Height&gt;100&lt;/Height&gt; &lt;/Position&gt; &lt;/Image&gt; </pre> | Image to display during the update process. You can specify the size and position of the image  |
| <pre> &lt;Rescan&gt; &lt;Count&gt;20&lt;/Count&gt; &lt;Delay&gt;2000&lt;/Delay&gt; &lt;/Rescan&gt; </pre>  | <p>Once a product is updated, the Firmware Updater waits for it to reboot and be re-enumerated by Windows.</p> <p>The Firmware Updater rechecks <b>Count</b> number of times for the product during this period, with a delay of <b>Delay</b> milliseconds between each check.</p> <p>If the product does not appear after this period, the Firmware Updater assumes something has gone wrong with the update.</p> <p>You can change these values to optimize the operation for your product, as the time taken to return may be specific to your product configuration</p> |
| <pre> &lt;/Branding&gt; </pre>   | End of the branding file  |

## Message box types

The Messages section of the branding file (see [<Messages>](#) on page 54) contains a MessageType value to control the appearance and content of each Windows message box you want to display. The value is defined by Windows, and is made of a combination of flags. The value for MessageType is derived from adding one value from each of the following tables.

Select one of the following flags to indicate the buttons contained in the message box.

| Value      | Description                          |
|------------|--------------------------------------|
| 0x00000000 | OK button only. This is the default. |
| 0x00000001 | OK and Cancel buttons                |
| 0x00000004 | Yes and No buttons                   |

Select one of the following flags to display an icon in the message box.

| Value      | Description                     |
|------------|---------------------------------|
| 0x00000030 | Exclamation-point icon          |
| 0x00000040 | Lower case letter i in a circle |
| 0x00000020 | Question-mark icon              |
| 0x00000010 | Stop-sign icon                  |

## Branding for Different Languages

The Firmware Updater user interface can support several languages: you create a branding file for each language you want. The Firmware Updater automatically displays the language that matches the Windows culture settings of the PC.

You can include identifiers for the language, or for the language and country, in the branding file name as follows:

```
branding_<language>.xml
branding_<language>_<country>.xml
```

The *language* identifier is a two to four letter code specified by ISO 639. For more details, see [http://en.wikipedia.org/wiki/ISO\\_639](http://en.wikipedia.org/wiki/ISO_639). The shortest code available for a language is used (e.g. **en** for English).

The *country* identifier is defined by ISO 3166. For more details, see [http://en.wikipedia.org/wiki/ISO\\_3166](http://en.wikipedia.org/wiki/ISO_3166).

The Firmware Updater selects the most appropriate branding file for the current regional settings in Windows. The Firmware Updater first looks for a branding file that contains both language and country code. If this is not found, the Firmware Updater looks for a branding file that contains just the language code. For example, when the Brazilian Portuguese Windows regional settings are in use ((language **pt**, country **BR**), the Firmware Updater looks for files in the following order:

- 1 A branding file called **branding\_pt\_BR.xml**.
- 2 If this is not present, a branding file called **branding\_pt.xml**.
- 3 If neither of these files is present, the Firmware Updater uses the default branding file **branding.xml**.

Branding files for different languages can specify features and user interface appearance details that are different from those in branding.xml or from other language branding files.

When translating the Firmware Updater user interface into other languages, follow these guidelines:

- Before starting any translation, ensure you have completed the customization and branding for your default branding.xml file. This minimizes the amount of rework for each translated language
- When translating text, only translate the displayed text. Do not translate control flags or XML tags

## Creating a Firmware Updater Package for Windows

When redistributing the Firmware Updater for Windows, you do not create a full installer, as it is a “run once” application, and not to be installed under Program Files.

One way to distribute the Firmware Updater is to create a self-extracting zip file that unzips the content of the 32-bit folder to a temporary folder and runs FirmwareUpdater.exe. The Firmware Updater automatically runs the DriverInstaller.exe application if it detects that the required device drivers are not available.



The 32-bit Firmware Updater supports operation on both 32- and 64-bit Windows.

For creating a self-extracting zip executable, we recommend the Chilkat freeware Zip 2 Secure EXE.

## Creating a Firmware Updater Package for Apple Macintosh

When redistributing the Firmware Updater for the Apple Macintosh, you must create a disk image (dmg) to ensure the required device drivers are installed. We provide a PackageMaker project, from which you create your customized dmg file. The PackageMaker file, called **Package.pmdoc**, is in the root of the RedistributableFiles folder you copied to your host when you installed the ISIS toolkit.

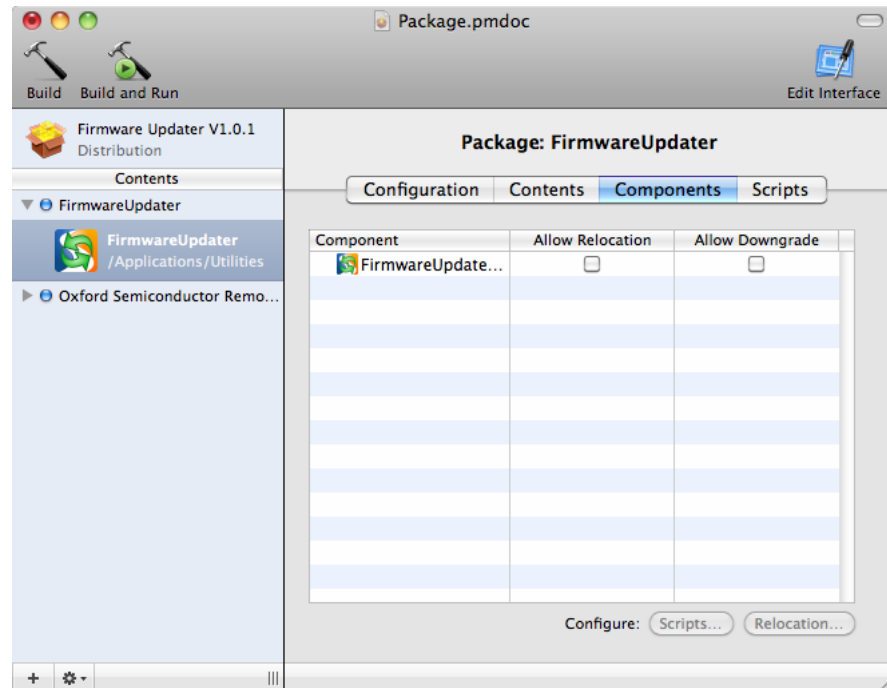


To open this file, you must have Xcode 3.2 installed. If you do not have Xcode installed, this appears as a normal folder. In this case, download and install Xcode 3.2 before continuing. After installing Xcode, you must initialize PackageMaker by running PackageMaker once from the Xcode Utilities folder. You can then open the folder by double-clicking.

Make the changes you want to the Gateway executable package, then create your own dmg file. To do so:

- 1 In the RedistributableFiles folder, double-click Package.pmdoc. The message **Resources Found** is shown.
- 2 Select **Do Not Use**.
- 3 Expand the FirmwareUpdater in the left hand column and select the FirmwareUpdater application.

- 4** In the Components tab, ensure **Allow Relocation** is unchecked. The generated package does not work if you leave this option checked.

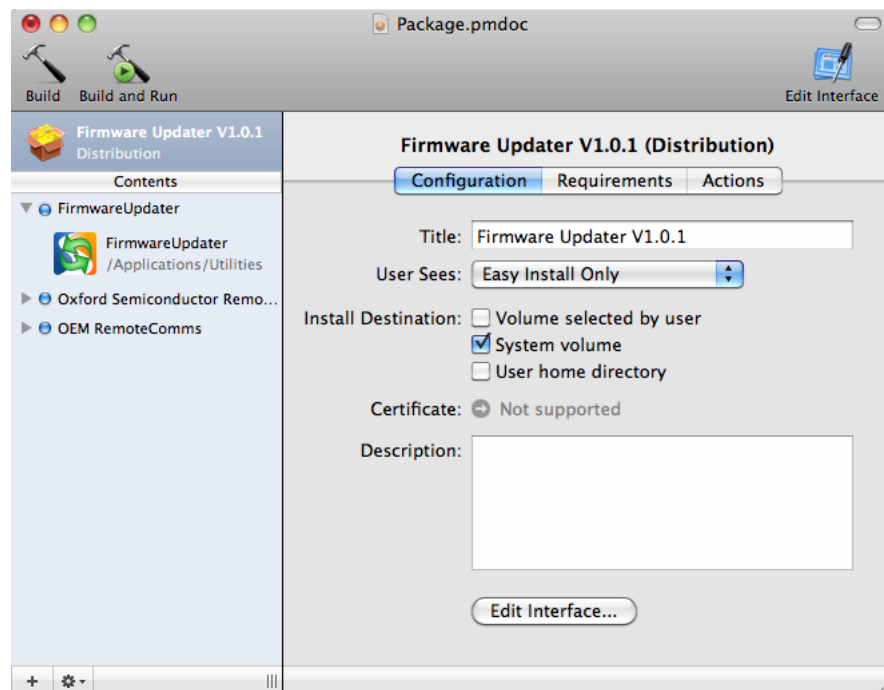


- 5 Make any other changes you require to the package, such as version number, displaying a readme file, or further company-specific branding. For more details, see the [PackageMaker documentation](#).
- 6 Click **Build**. Select the location to save the dmg file in and click **Save**.

If you change the vendor ID string returned for a SCSI inquiry command from the default value of “OEM “, you must:

- Specify this value in the branding file (see [Changing SCSI vendor information on an Apple Macintosh](#) on page 31)
- Create a customer-specific RemoteComms driver layer and add it to this package. For details of creating the driver layer, see Chapter 7 [Creating a RemoteComms Driver Layer for Apple Macintosh](#)

To add your driver layer to the disk image for your Firmware Updater package, click the **+** button at the bottom left of PackageMaker and select your driver layer. This example shows a driver layer package called OEM RemoteComms.



This page is intentionally blank

## Creating a RemoteComms Driver Layer for Apple Macintosh

If you change the vendor ID string returned for a SCSI inquiry command from the default value of OEM, you must also create a custom RemoteComms driver layer, and add it to your redistributable package.

To create the driver layer, ensure you copied the file **MyCompanyName\_RemoteCommsSample\_Vw\_xx\_yyyy\_zzzz.zip** to your host when installing the ISIS toolkit (see [Installing the ISIS Toolkit](#) on page 3). This file contains everything you need to create the driver layer. You must have Xcode 3.2 installed on your host.

To create the driver layer, you create an Xcode project, from which you create the driver layer. To create the Xcode project:

- 1 Unzip the **MyCompanyName\_RemoteCommsSample\_Vw\_xx\_yyyy\_zzzz.zip** file to a folder on your host.
- 2 Go to the Utilities folder on your Apple Macintosh and open the Macintosh Terminal utility.
- 3 Change directory (cd) to the folder where you unzipped the file.
- 4 Run the file **rename.sh**, as follows:

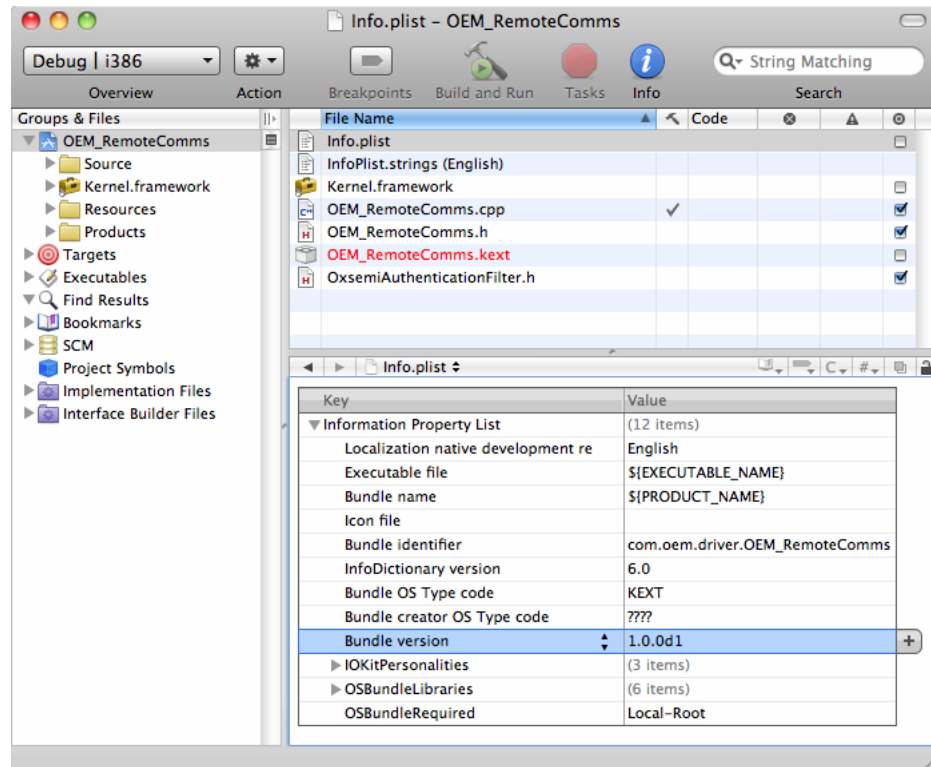
```
./rename.sh CompanyName "CompanyVid"
```

where:

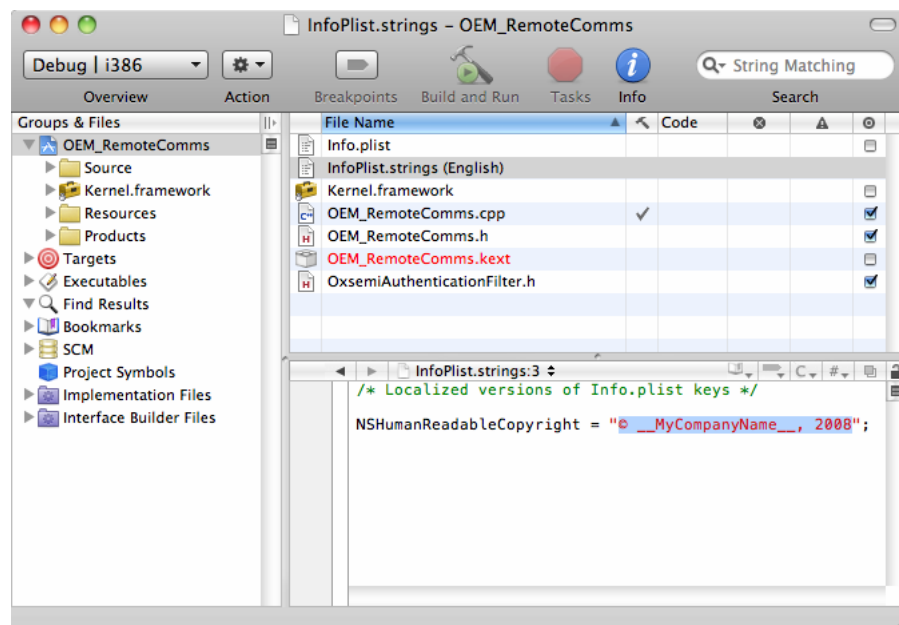
- *CompanyName* is a short name for your company (no spaces allowed)
- *CompanyVid* is the SCSI vendor ID string returned by your device. If your vendor ID string ends with multiple spaces, only enter one in this string. Hence in this example, for a company called OEM, with a device returning a SCSI vendor ID string of **oem\_** (where **\_** is a space), you type:  
**./rename.sh OEM "oem\_"**

This creates a subfolder containing your driver layer project, and displays instructions on the next steps required. In this example the folder is called OEM.

- 5 Open the driver layer folder in Finder and double-click the Xcode project; in this example, OEM\_RemoteComms.xcodeproj. This opens the project in Xcode.
- 6 You must change the bundle version in **Info.plist** to meet your own requirements.



- 7 You must change the copyright text in **InfoPlist.strings** to meet your own requirements.





- 8** Change the target at the top left to a Release build, and select **Build**. This creates your driver kext file in the build\Release subfolder. In this example, the file is called OEM\_RemoteComms.kext.
- 9** In the Terminal window, change directory (cd) to the folder containing your kext file. Change the ownership of this kext file, in this example:  
`sudo chown -R root:wheel OEM_RemoteComms.kext`
- 10** When prompted, enter your account password.

To include your RemoteComms driver layer in your redistributable package, see [Creating a Gateway Package for Apple Macintosh](#) on page 41 and [Creating a Firmware Updater Package for Apple Macintosh](#) on page 59.

This page is intentionally blank