

# ***Odyssey<sup>®</sup> CA***

## ***Administration Guide***

***First Edition***

***October, 2004***

Funk Software, Inc.  
222 Third Street  
Cambridge, MA 02142

(617) 497-6339  
(617) 491-6503 (Technical Support)  
[www.funk.com](http://www.funk.com)

© Copyright 2003-2004 Funk Software, Inc. All rights reserved. Odyssey CA ©2003-2004 Funk Software, Inc. All rights reserved. Odyssey® and Funk® are registered trademarks of Funk Software, Inc. Microsoft, Windows, Windows NT, Windows 2000, Internet Explorer, and other Microsoft products referenced herein are either trademarks or registered trademarks of the Microsoft Corporation in the United States and other countries. Java is a trademark of Sun Microsystems, Inc. Portions copyright (c) 2000, The Apache Software Foundation. All rights reserved. Portions copyright (c) 2000, The Legion Of The Bouncy Castle. All rights reserved.

# Contents

## Chapter 1 Introduction

Welcome .....	1
Operating system requirements .....	1
Documentation .....	2
Technical support .....	2
Odyssey Certificate Requester .....	3

## Chapter 2 Installation

Installing Odyssey CA installation .....	5
--	---

## Chapter 3 Using Odyssey CA

Odyssey CA Administrator .....	7
Odyssey CA Administrator basics .....	8
Create or configure a certificate authority .....	10
Settings .....	11
Default certificate duration .....	11
Pending Certificate Requests .....	12
Refresh .....	12
Process .....	12
Deny .....	14
Completed Certificate Requests .....	14
Certificates .....	15
View certificates .....	16
Revoke certificates .....	16
Refresh certificates .....	17
Pending CRL Operations .....	17
Refresh pending operations .....	18
View certificate records .....	18
Undo status change actions .....	18
CRL Schedule .....	18
Add a certificate revocation list generation schedule .....	19

Edit a certificate revocation list generation schedule .....	20
Remove a certificate revocation list generation schedule .....	20
Generate a certificate revocation list .....	20
Revoked Certificates .....	20
Refresh revoked certificates .....	21
View a revoked certificate .....	22
Restore revoked certificates .....	22
Menus.....	22
File menu .....	23
Help menu .....	23
<b>Index .....</b>	<b>25</b>

# Chapter 1

## Introduction

### Welcome

Thank you for selecting the certificate authority, Odyssey<sup>®</sup> CA. You can use Odyssey CA to create and deliver server authentication certificates for Odyssey Server and Steel-Belted Radius. You can use Odyssey CA to create a single certificate authority, or a CA that belongs to a hierarchy of CAs.

In concert with the Odyssey Certificate Requester, you can use Odyssey CA for the following tasks:

- ▶ Create a root certificate authority or an intermediate certificate authority.
- ▶ Issue certificates or deny certificate requests.
- ▶ Revoke issued certificates.
- ▶ Restore revoked certificates.
- ▶ Configure schedules for automatically generated certificate revocation lists.
- ▶ Manually generate a certificate revocation list.

See also the following informational topics:

- ▶ [Operating system requirements](#)
- ▶ [Documentation](#)
- ▶ [Technical support](#)
- ▶ [Odyssey Certificate Requester](#)

### Operating system requirements

Odyssey CA runs under the following operating systems:

- ▶ Windows 2000 Server

- ▶ Windows 2000 Advanced Server
- ▶ Windows 2000 Professional
- ▶ Windows XP Professional
- ▶ Windows 2003 Server

**NOTE:** *Service Pack 2 is required for all editions of Windows 2000.*

## Documentation

This manual, and the README.TXT file included with the software, provide all the information that you need to configure and use Odyssey CA.

Odyssey CA includes a help system that allows you to access this documentation from the **Help** menu. You can also get context-sensitive help at any time by pressing **F1** on your keyboard.

To open the README.TXT file in a text editor, select the file from the in the product directory once you install the product. The default location of this directory is Program Files\Funk Software\ODCA.

## Technical support

If you have any problems installing or using Odyssey CA, there are various resources available to help you at no charge:

- ▶ This manual, along with the README.TXT file, may contain the information you need to solve the problem you are having. Please re-read the relevant sections — you may find a solution you overlooked.

To view the readme.txt file, double-click this file that is located in the product install directory after you install the product.

- ▶ Check our web site — <http://www.funk.com> — for additional information and technical notes.
- ▶ E-mail your questions or issues to [support@funk.com](mailto:support@funk.com).
- ▶ Our technical support staff is available to assist you on weekdays between 9:00 AM and 5:30 PM Eastern Time at (617) 491-6503.

**NOTE:** *Odyssey CA is intended for use with Odyssey Server and Steel-Belted Radius. Any other use is prohibited. We can only offer support to users of Steel-Belted Radius or Odyssey Server who are entitled to support.*

If you are located outside North America, you can receive support either by contacting the Funk Software partner in your country or by contacting us directly. You can find the name of the support provider nearest you on our web site — from our home page, navigate to **Contact Info > International**.

## Odyssey Certificate Requester

Odyssey CA is a companion product for the Odyssey Certificate Requester:

- ▶ You can use Odyssey CA to issue or deny certificate requests that are made by an administrator using Odyssey Certificate Requester. The default installation directory for Odyssey Certificate Requester (`odCertificateRequester.exe`) is `C:\Program Files\Funk Software\Odyssey Requester`.
- ▶ You can use the Odyssey Certificate Requester in order to configure certificates for use with Odyssey Server or Steel-Belted Radius. You must run the Odyssey Certificate Requester on the same machine on which you have installed Odyssey Server or Steel-Belted Radius.



# Chapter 2

## Installation

### Installing Odyssey CA installation

Odyssey CA requires Java Runtime Environment, which you can install for free as part of the installation process.

To install Odyssey CA, double-click the file `Odyssey CA.msi`, located in the CA directory of the CD. If you download Odyssey CA from our website, double-click the download file `Odyssey CA.msi`, in order to begin the installation process.

***NOTE:*** *You must have administrative privileges on the machine in order to install Odyssey CA.*



# Chapter 3

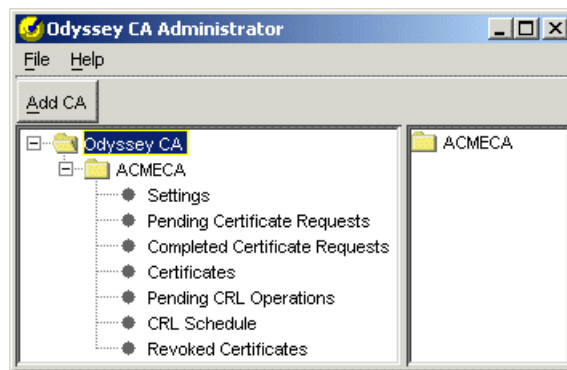
## Using Odyssey CA

### Odyssey CA Administrator

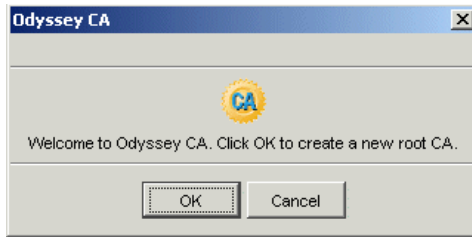
You can use the Odyssey CA to create certificate authorities through which you can issue or deny certificate requests that are initiated by the [Odyssey Certificate Requester](#).

You can configure Odyssey CA using the **Odyssey CA Administrator**.

To start the **Odyssey CA Administrator**, select **Start > Programs > Funk Software > Odyssey CA > Odyssey CA Administrator** from the Windows taskbar.



The first time you use Odyssey CA you are offered the option to create a CA immediately.



If you want to create a new certificate authority, click **OK** and follow the instructions according to [“Create or configure a certificate authority” on page 10](#). Before you can issue certificates or deny certificate requests made by Odyssey Certificate Requester, you must first create a CA. You can create a single CA, or you can create a CA that belongs to a hierarchy of CAs.

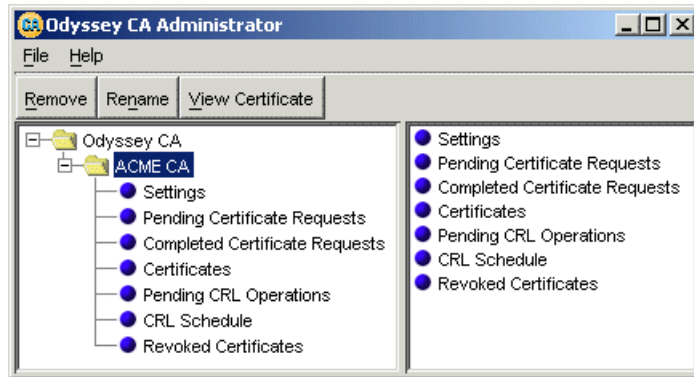
See [“Odyssey CA Administrator basics” on page 8](#) for information on navigating Odyssey CA.

Once you create a CA for your machine on which you have installed Odyssey CA, you can use the following Odyssey CA features:

- ▶ **Settings**, for modifying the default duration of all certificates you issue
- ▶ **Pending Certificate Requests**, for issuing or denying pending requests
- ▶ **Completed Certificate Requests**, for viewing detailed results of your treatment of pending requests
- ▶ **Certificates**, for viewing a listing of all certificates you issue
- ▶ **CRL Schedule**, for creating a schedule for automatic generation of certificate revocation lists
- ▶ **Revoked Certificates**, for viewing information about revoked certificates, as well as for restoring revoked certificates to valid status

## Odyssey CA Administrator basics

When you start the Odyssey CA, the **Odyssey CA Administrator** appears.



Observe the following:

- ▶ **Odyssey CA** is listed as the top item on the left folder panel. As soon as you add a certificate authority, it appears as a subfolder on the left, with a number of function folders below it. These folders appear in the right panel when you select a certificate authority without expanding it.
- ▶ Each of the function folders represents a sequence of possible actions that you can undertake, or information items that you can view. These function folders become populated and/or emptied as you move through the process of granting, denying, or revoking a certificate.
- ▶ The action buttons appear above the folders panel. These buttons change as you select different items in this panel. For example, when you select **Odyssey CA**, you can add a new certificate authority. In addition, the informational display changes in the data panel for each function folder you select.
- ▶ All folder actions are available to you via the action buttons above the panels, or by using a right-click menu from selected items.
- ▶ Items that appear in function folders are represented by a set of information headings that vary with each folder. For example, pending certificate requests are marked with the **Thumbprint** and **Subject** of the certificate. You can resize the column headings. You can also resort the displayed information when you click a column heading. The resulting sort is alphabetical with respect to the information listed under the selected column heading.

## Create or configure a certificate authority

You can use Odyssey CA to create or configure a certificate authority using either of the following methods:

- ▶ Configure a certificate authority from a certificate that you import from a `.pfx` file.
- ▶ Create a new root certificate authority, along with its certificate.
- ▶ Create a new intermediate certificate authority (along with its certificate) that is subordinate to (issued by) a CA that is already configured in **Odyssey CA Administrator**.

To create or configure a new certificate authority using either of these methods, select **Odyssey CA**, and click **Add CA**. The **Add CA** wizard appears.

You can use the **Add CA** wizard to specify all of the components of your certificate, such its name, common name, and key algorithm.

Follow each of the **Add CA** wizard screens:

- ▶ Follow the instructions on each screen.
- ▶ Supply the required information for each screen.
- ▶ Supply any optional information.
- ▶ Click **Next**, to continue through the wizard.
- ▶ Click **Back**, to review or revise your configuration before your finish the wizard.
- ▶ Click **Finish** at the last screen, to complete your CA configuration.

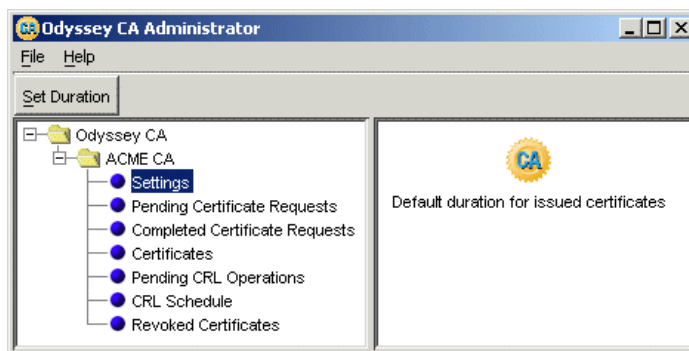
Note the following:

- ▶ *The only type of intermediate CAs that you can create are ones subordinate to a CA created on your local machine with Odyssey CA, or ones subordinate to a CA that is imported to Odyssey CA through a `.pfx` file. You must already have created the root (and chained intermediate) certificate authority in order to add a new intermediate CA.*
- ▶ *You must select a key algorithm and a digest algorithm for each CA you create.*
- ▶ *When you import a certificate from a `.pfx` file, you must know both the `.pfx` file password, and the private key password.*

Once you have created the certificate authority, you can view its details in the **Odyssey CA Administrator**.

# Settings

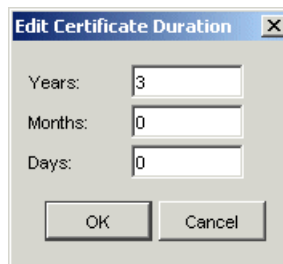
You can set the default duration for issued certificates in the **Settings** folder.



## Default certificate duration

Every certificate that you issue has an expiration date. This value is the date of issuance, plus a duration that you configure in the CA. Initially, the default value for the duration is one year.

You can change the default duration for any new certificates that you issue from your CA by clicking **Set Duration**.

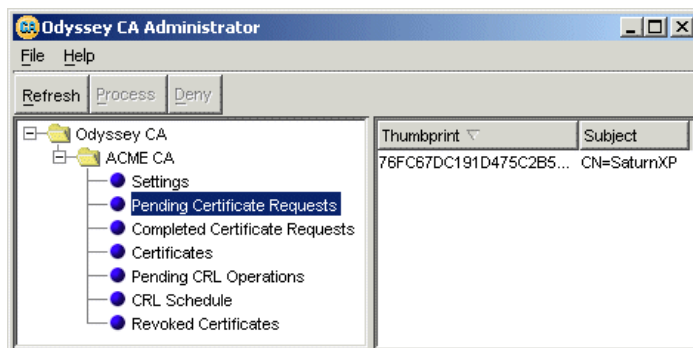


Fill in the number of years, months, and days (as whole numbers) for the default certification duration, and click **OK**.

Note that you can always modify this default duration of any certificate when you issue it. See [“Process” on page 12](#).

# Pending Certificate Requests

Whenever the [Odyssey Certificate Requester](#) sends a request for a certificate to the Odyssey CA, such requests appear in the **Pending Certificate Requests** folder.



You can take the following actions in this folder:

- ▶ **Refresh**
- ▶ **Process**
- ▶ **Deny**

## Refresh

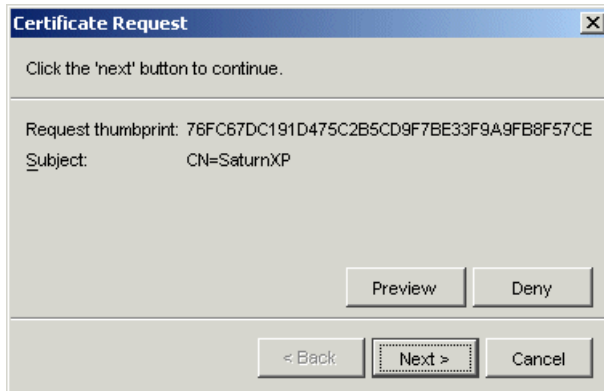
If you know that a certificate request has been made to your Odyssey CA, but you are unable to view any items in the **Pending Certificate Requests** folder, select this folder, and click **Refresh**. Any new certificates requests appear in the right-hand panel.

## Process

Pending certificate requests arise when the [Odyssey Certificate Requester](#) sends a request for a server certificate.

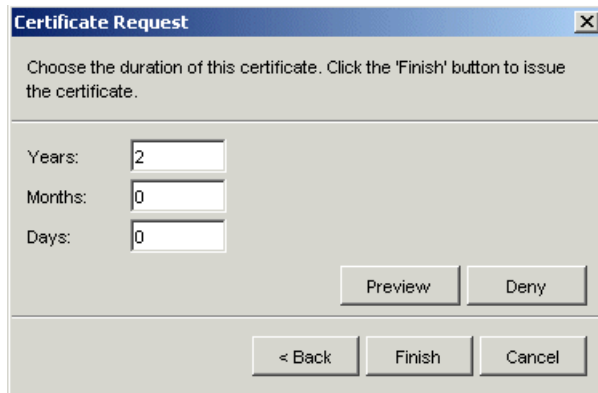
To process a pending certificate request, follow these steps:

- 1 Double-click the certificate request you want to process. The **Certificate Request** dialog appears.



2 You have five choices:

- ▶ Click **Preview** if you want to view the details of the certificate request.
- ▶ Click **Deny** to deny the request.
- ▶ Click **Next**, if you want to issue the certificate. When you do so, you can configure the duration (in whole numbers) for the certificate, and click **Finish** to complete the process.



- ▶ Click **Back** to return to the previous screen.
- ▶ Click **Cancel**, if you do not want to process the request at this time.

Once you either issue the certificate or deny the request, the certificate request is no longer pending, and the following occurs:

- ▶ The request is removed from the **Pending Certificate Requests** folder.

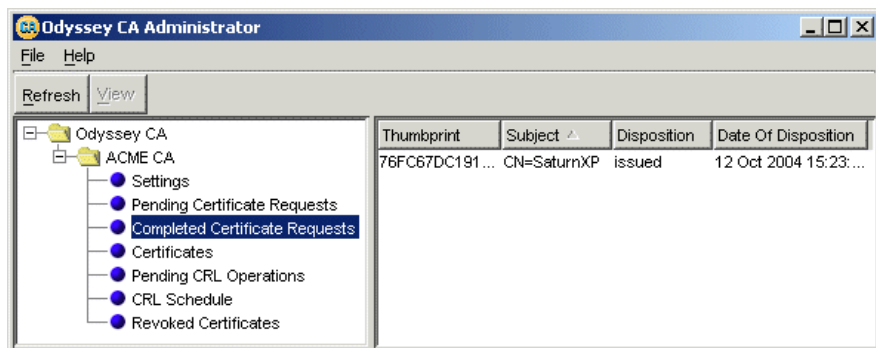
- ▶ The a record of the processed certificate appears in the **Completed Certificate Requests** folder as well as the **Certificates** folder.

## Deny

You can deny a certificate request directly by selecting the certificate request in the **Pending Certificate Requests** folder, and clicking **Deny**.

## Completed Certificate Requests

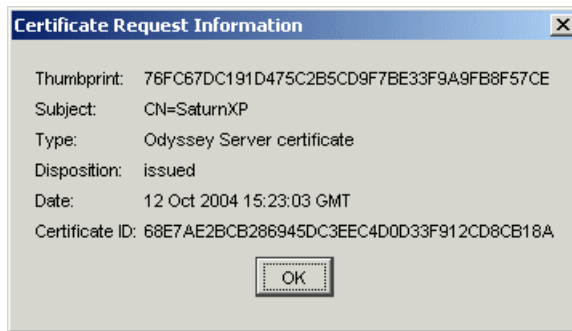
Any certificates that you process with a given certificate authority appear in the **Completed Certificate Requests** folder.



If this folder is empty when you have completed a pending request, you can click **Refresh** in order to update the folder.

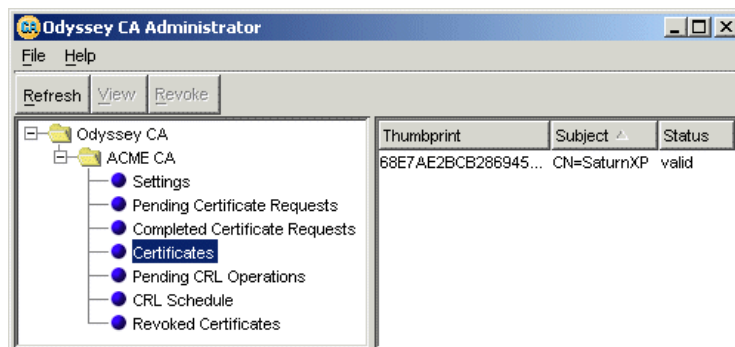
In addition to the **Thumbprint** and **Subject** fields that are visible to the pending certificate requests, issued or denied certificates that are displayed in this folder have a **Disposition** field. The disposition indicates your processing action for the certificate (**issued** or **denied**).

To view more detailed information on a completed certificate, double-click the certificate of interest or select the certificate, and click **View**.



## Certificates

Every certificate that you issue has a record in the **Certificates** folder.



In addition to **Thumbprint** and **Subject** fields, certificate records that are in this folder have a **Status** field that corresponds to the certificate status.

There are three possible status values:

- ▶ valid
- ▶ expired
- ▶ revoked

You can undertake three actions in this folder:

- ▶ View certificates
- ▶ Revoke certificates
- ▶ Refresh certificates

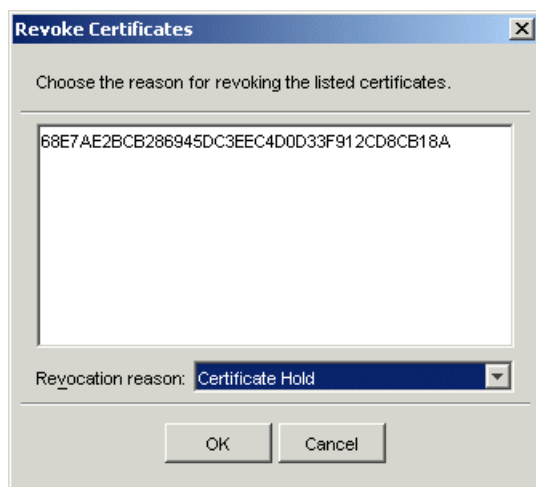
## View certificates

To view a certificate in the certificates folder, double-click the certificate of interest. You can view general information, detailed information, and status information when you do so.

## Revoke certificates

It may be necessary for you to revoke a certificate.

To revoke a certificate, select the certificate (or certificates) of interest, and click **Revoke**. **Revoke Certificates** appears.



In order to revoke a certificate, you must specify a reason. Select a reason from those provided in the drop-down list, and click **OK**.

This certificate revocation action takes effect as soon as you generate a CRL. Before you do so, the certificate record populates the **Pending CRL Operations** panel. The **Operation** field of this record reflects the **revoke** action you intend to enact.

Once you generate a CRL, the revoke action is enacted.

If you revoke a certificate, the status of its record in the **Certificates** panel is changed to **revoked**. If you restore a revoked certificate, the status of its record in the **Certificates** panel is reverted to **valid**.

## Refresh certificates

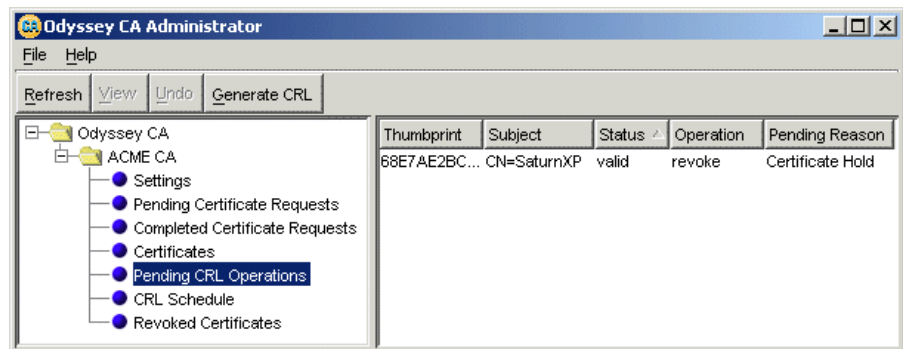
If your certificate revocation list happens to generate (as per a CRL schedule) when you have your **Certificates** folder open, it is possible that status changes occur to individual certificates in this folder. You can check the latest status of the certificates in **Certificates**, by clicking **Refresh**.

## Pending CRL Operations

You can undertake two actions that change the status of a certificate:

- ▶ Revoke certificates in the **Certificates** folder.
- ▶ Restore revoked certificates in the **Revoked Certificates** folder.

Once you undertake an action to change the status of a certificate, it appears in the **Pending CRL Operations** folder.



This folder is emptied of all pending items every time you generate a certificate revocation list.

You can perform the following actions using the buttons that are located at the top of the panel:

- ▶ Refresh pending operations.
- ▶ View certificate records.
- ▶ Undo status change actions.
- ▶ Generate a certificate revocation list. (See “[Generate a certificate revocation list](#)” on page 20 for more information.)

## Refresh pending operations

If your certificate revocation list happens to generate when you have your **Pending CRL Operations** folder open, it is possible that status changes occur to individual pending operations that are displayed in this folder. You can check the latest status of the certificates in **Pending CRL operations**, by clicking **Refresh**.

## View certificate records

To view any certificate records listed in this panel, double-click the record of interest. You can also select the record and click **View**.

## Undo status change actions

Items in the **Pending CRL Operations** folder have one of the following two status values:

- ▶ **Revoked**, for certificates that are pending revocation
- ▶ **Restored**, for revoked certificates that are pending restoration as valid

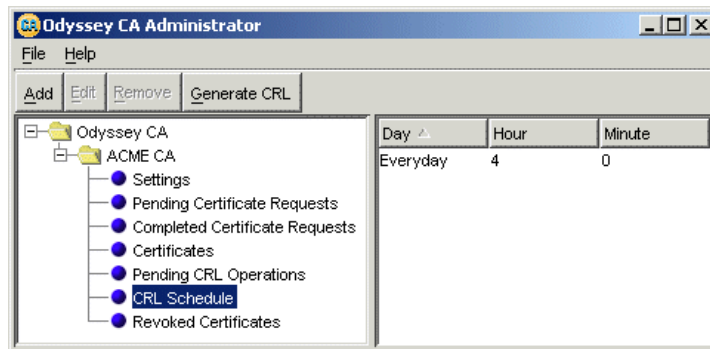
You can revert the pending status by selecting a certificate (or a group of certificates), and clicking **Undo**. The following changes occur to all selected items:

- ▶ Any certificates that are pending revocation are retained as valid.
- ▶ Any revoked certificates that pending restoration remain revoked.
- ▶ The selected items are no longer pending.

Note that you must perform the **Undo** operation before you generate a CRL, as that action empties the **Pending CRL Operations** folder.

## CRL Schedule

Certificate revocation lists (CRLs) are used to publish revocation and restore actions that you process in the **Odyssey CA Administrator**.



You can undertake the following CRL actions in the **CRL Schedule** folder:

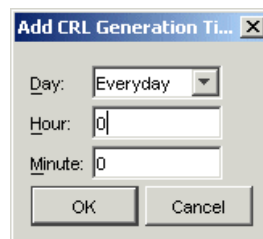
- ▶ Add a certificate revocation list generation schedule
- ▶ Edit a certificate revocation list generation schedule
- ▶ Remove a certificate revocation list generation schedule
- ▶ Generate a certificate revocation list

## ***Add a certificate revocation list generation schedule***

The certificate revocation list generation schedules determine the times at which the CRL is generated. You can create more than one schedule, depending on your daily requirements for CRL generation.

To add a CRL generation list schedule, follow these steps in the **CRL Schedule** folder:

- 1** Click **Add**. The **Add CRL Generation Time** dialog appears.

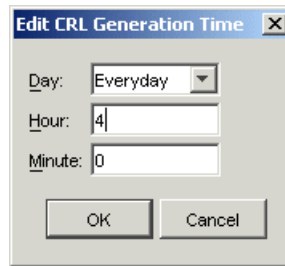


- 2** Select **Everyday** from the list if you want this CRL to be generated daily at a specific time. Otherwise, select a day of the week from the list.
- 3** Type in a two-digit hour for 24 hour clock.

- 4 Type in a two-digit minute value.
- 5 Click **OK**.

## ***Edit a certificate revocation list generation schedule***

To edit a certificate revocation list generation schedule, double-click the schedule of interest that is located in the **CRL Schedule** folder. The **Edit CRL Generation Time** dialog opens.



Edit your settings as desired, and click **OK**.

## ***Remove a certificate revocation list generation schedule***

To remove a certificate revocation list generation schedule, select the schedule (or schedules) of interest, and click **Remove**.

## ***Generate a certificate revocation list***

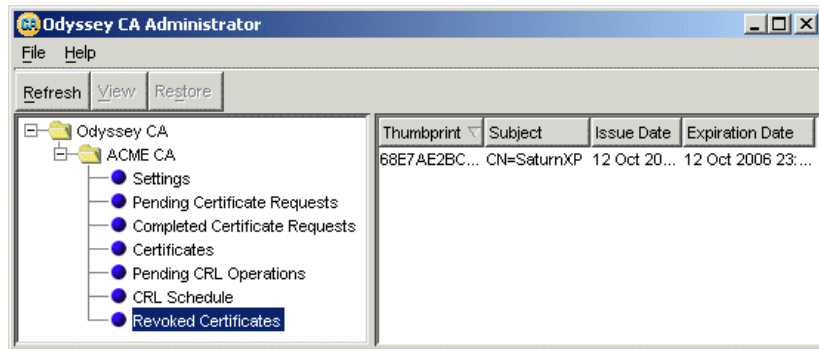
You may want to generate a certificate revocation list immediately, rather than wait for the CRL schedule to take effect.

To generate a certificate revocation list, click **Generate CRL**.

When you do so, the status of all affected certificates is updated in the **Certificates** panel. In addition, the **Pending CRL Operations** panel is emptied of pending items.

## **Revoked Certificates**

You can view a listing of all revoked certificates in the **Revoked Certificates** panel.



You can undertake the following actions in this panel:

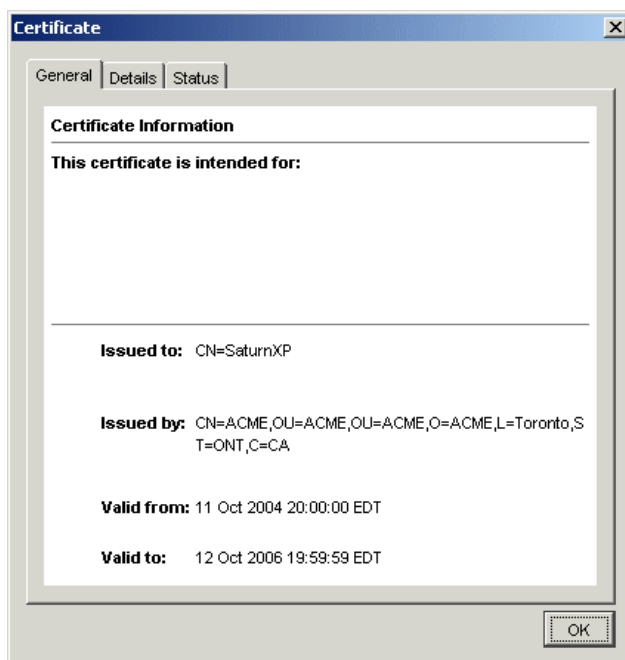
- ▶ Refresh revoked certificates
- ▶ View a revoked certificate
- ▶ Restore revoked certificates

## ***Refresh revoked certificates***

You may need to refresh the **Revoked Certificates** panel in order to update its contents. To do so, click **Refresh**.

## View a revoked certificate

You can view any revoked certificate by double-clicking it.



## Restore revoked certificates

You can restore any certificate whose record is listed in the **Revoked Certificates** panel. To restore one or more certificates, select the certificate (or a set of certificates) of interest, and click **Restore**.

Once you click **Restore**, the certificate record populates the **Pending CRL Operations** panel, and the **Operation** field reflects the **restore** action. This record remains in the **Pending CRL Operations** panel, until you generate a new certificate revocation list (or one is generated on schedule).

## Menus

There are two menus for the **Odyssey CA Administrator**:

- ▶ File menu
- ▶ Help menu

## ***File menu***

You can exit the **Odyssey CA Administrator** from the **File** menu. Select **Exit** from this menu in order to do so.

## ***Help menu***

You can select from two menu items:

- ▶ Help Topics
- ▶ View Readme File
- ▶ About Odyssey CA

### **Help Topics**

Select **Help Topics** to open the help file.

You can use the following online help features to learn about the product:

- ▶ Table of contents
- ▶ Index
- ▶ Keyword search

### **View Readme File**

Select **View Readme File** to open the ReadMe.txt file.

### **About Odyssey CA**

Select **About Odyssey CA**, in order to view version and copyright information.



## A

- about page 1
- adding
  - certificate authorities 10
  - certificate revocation list schedules 19
  - intermediate CAs 10
- administering Odyssey CA 7

## C

- certificate authorities, adding 10
- certificate revocation lists
  - generating 20
  - schedules
    - adding 19
    - editing 20
    - removing 20
- certificates
  - default duration, setting 11
  - folder 15
  - pending 17
  - refreshing 17
  - requests for
    - completed 14
    - denying 14
    - issuing 13
    - server, from 3
  - restoring 22
  - revoked, listing of 20
  - revoking 16
- completed certificate requests folder 14
- copyright information 1
- CRL
  - operations, pending 17
  - schedules 18

## D

- deny pending requests 14
- documentation 2
- duration, setting default for certificates 11

## E

- editing CRL schedules 20

## F

- Funk Software, Inc. information 1

## G

- generating certificate revocation lists (CRLs) 20
- getting help 23

## H

- help, getting 23

## I

- installation
  - certificate authority, new 10
  - overview 5
  - product, of 5
  - requirements 5
- intermediate CAs, creating 10
- introduction to the product 1

## M

- menus 22

## O

- Odyssey CA
  - administering 7
  - overview 8
- Odyssey Certificate Requester 3

## P

- pending
  - certificate requests
    - folder 12
    - processing 12
    - refresh 12
  - CRL operations 17
- processing pending certificate requests 12
- product requirements 1

## R

- refresh certificates 17
- refreshing
  - pending certificate requests folder 12
  - pending CRL operations 18
  - revoked certificates folder 21
- removing CRL schedules 20
- requester 3
- requests
  - making 3
  - pending 12
  - processing 12
- requirements for the product 1
- restoring revoked certificates 22
- revoked certificates
  - creating 16
  - folder 20
  - refreshing 21
  - restoring 22
  - viewing 22

## S

- scheduling CRLs 19
- settings
  - CRL 18
  - folder 11
- support, accessing 2

## T

- technical support 2

## U

- undo button, pending CRL operations 18

## V

- viewing
  - pending CRL operations 18
  - revoked certificates 22