Agent’s Guide

Sun™ ONE Certificate Server

4.7

September 2002
816-5543-10
Second Edition

THIS DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) "HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT "LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

CETTE DOCUMENTATION EST FOURNIE "EN L'ÉTAT", ET TOUTES CONDITIONS EXPRESSES OU IMPLICITES, TOUTES REPRÉSENTATIONS ET TOUTES GARANTIES, Y COMPRIS TOUTE GARANTIE IMPLICITE D'APTITUDE À LA VENTE, OU À UN BUT PARTICULIER OU DE NON CONTREFAÇON SONT EXCLUES, EXCEPTÉ DANS LA MESURE OÙ DE TELLES EXCLUSIONS SERAIENT CONTRAIRES À LA LOI.

Contents

About This Guide

This guide describes the Agent Services interface that a Sun™ ONE Certificate Server agent uses to administer a subsystem's certificates and keys.

NOTE Sun™ ONE Certificate Server was previously known as iPlanet™ Certificate Management System. The product was renamed shortly before the launch of this 4.7 release.

The late renaming of this product has resulted in a situation where the new product name is not fully integrated into the shipping product. In particular, you will see the product referenced as iPlanet Certificate Management Server (CMS) within the product GUI and within the product documentation. For this release, please consider iPlanet Certificate Management Server and Sun™ ONE Certificate Server as interchangeable names for the same product.

This preface has the following sections:

- What You Should Already Know (page 5)
- What's in This Guide (page 6)
- Conventions Used in This Guide (page 7)
- Where to Go for Related Information (page 8)

What You Should Already Know

This guide is intended for Certificate Management System agents—that is, privileged users designated by the Certificate Management System administrator to manage requests from end entities for certificate-related services. Each installed CMS manager (Certificate Manager, Registration Manager, and Data Recovery Manager) can have one or more agents.

Server administrators should refer to the *CMS Agent’s Guide* for information on how to designate agents and assign agent privileges to users and groups.

Before reading this guide, you should be familiar with the basic concepts of public-key cryptography and the Secure Sockets Layer (SSL) protocol. These include the following topics:

- Encryption and decryption
- Public keys, private keys, and symmetric keys
- Digital signatures
- The role of digital certificates in a public-key infrastructure (PKI)
- Certificate hierarchies
- SSL cipher suites
- The purpose of and major steps in the SSL handshake

For overviews of these topics, see Appendix D and Appendix E of *Managing Servers with iPlanet Console*.

What’s in This Guide

This guide describes the duties of the agents for the various CMS subsystems and explains how to accomplish each task.

- Chapter 1, “Agent Services” provides an overview of the product and identifies the different kinds of users, including agents. The chapter also summarizes the tasks of each subsystem agent and lists the HTML forms you use to perform agent tasks. Finally, the chapter explains how to access the Agent Services pages and forms.
- As a Certificate Manager or Registration Manager agent, you are responsible for handling requests for certificates that are made by end entities (end users, server administrators, or other CMS subsystems) using manual enrollment. Chapter 2, “Handling Certificate Requests” describes the general procedure for handling requests and explains how to handle different aspects of certificate request management.

- Chapter 3, “Finding and Revoking Certificates” explains how, as a Certificate Manager agent, you can use the Agent Services page to find and examine a specific certificate issued by Certificate Management System, or retrieve a list of certificates that match specified criteria. This chapter also explains how to revoke certificates, and manage the certificate revocation list.
- Chapter 4, “Publishing to a Directory” describes how a Certificate Manager agent can update the LDAP directory with the current status of certificates.
- Chapter 5, “Recovering Encrypted Data” describes how to process key recovery requests, and how to recover stored encrypted data when the encryption key has been lost. This service is only available when the Data Recovery Manager subsystem is installed.
- Chapter 6, “Managing OCSP Service Related Tasks” describes how to handle tasks related to the CMS OCSP responder, Online Certificate Status Manager. This service is only available when the Online Certificate Status Manager subsystem is installed.

Conventions Used in This Guide

This guide uses the following conventions:

`Monospaced` font	This typeface is used for text that is an executable part of a program or text that you type. It’s also used for filenames, directory names, and URLs.
Italic	Italic type is used for emphasis, book titles, and to introduce new or glossary terms.
Text within “quotation marks”	Indicates cross-references to other topics within this guide.
Square brackets `[ ]`	Square brackets enclose commands that are optional.
Angle brackets <>	Angle brackets indicate placeholders for items that vary, such as pathnames and variable names. Replace the angle brackets and their text with text that applies to your situation.
Forward slash `/`	A slash is used to separate directories in a path. (Note that the Windows NT operating system supports both the slash and the backslash.)
Sidebar text	Sidebar text marks important information. Make sure you read the information before continuing with a task.

In addition, the following conventions are used for important notes.

NOTE	You can access the Agent Services only if you have a valid agent certificate.

CAUTION	A caution note documents a potential risk of losing data, damaging software or hardware, or otherwise disrupting system performance.

Where to Go for Related Information

This section summarizes the documentation that ships with Certificate Management System, using these conventions:

- `<server_root>` is the directory where the CMS binaries are kept (specified during installation).
- `<instance_id>` is the ID for this instance of iPlanet Certificate Management Server (specified during installation).

The documentation set for Certificate Management System includes the following:

- *Managing Servers with iPlanet Console*

  Provides background information on basic cryptography concepts and the role of iPlanet Console.

  To view the HTML version of this guide, open this file:
  `<server_root>/manual/en/admin/help/contents.htm`

- *CMS Installation and Setup Guide*

  Provides detailed information on deployment options for Certificate Management System, a walk-through of a test or demo installation, complete installation instructions, and information on administrative tasks. To access the installation and configuration information from within the CMS Installation Wizard, click any help button.

  To view the HTML version of this guide, open this file:
  `<server_root>/manual/en/cert/setup_guide/contents.htm`

- *CMS Plug-Ins Guide*

  Provides detailed reference information on CMS plug-ins for authentication, policy, publishing, and so on. To access this information from the CMS window within iPlanet Console, click any help button.

  To view the HTML version of this guide, open this file: `<server_root>/manual/en/cert/plugin_guide/contents.htm`

- *CMS Command-Line Tools Guide*

  Provides detailed reference information on CMS tools.

  To view the HTML version of this guide, open this file: `<server_root>/manual/en/cert/tools_guide/contents.htm`

- *CMS Customization Guide*

  Provides detailed reference information on customizing the HTML-based agent and end-entity interfaces.

  To view the HTML version of this guide, open this file: `<server_root>/manual/en/cert/custom_guide/contents.htm`

- *CMS Agent's Guide* (this guide)

  Provides detailed reference information on CMS agent interfaces. To access this information from the Agent Services pages, click any help button.

  To view the HTML version of this guide, open this file: `<server_root>/<instance_id>/web/agent/manual/agent_guide/contents.htm`

- End-entity help provides detailed reference information on CMS End-Entity Services interface. Users can access this guide by clicking any help button in the end user pages.

  To view the HTML version of this guide, open this file: `<server_root>/<instance_id>/web/ee/manual/ee_guide/contents.htm`

CAUTION Do not change the default location of any of the HTML files; they are used for the online help. You may move the PDF files to another location.

For a complete list of all documentation that ships with Certificate Management System, open this file: `<server_root>/manual/index.html`

You will not be able to access the files and directories specified here if you don't have access to the machine on which Certificate Management System is installed.

For the latest information about Certificate Management System, including current release notes, complete product documentation, technical notes, and deployment information, check this site: `http://docs.iplanet.com/docs/manuals/cms.html`

Chapter 1

Agent Services

This chapter describes the role of the privileged users called *agents* in managing iPlanet Certificate Management Server (CMS). It also introduces the tools that agents use to administer service requests.

The chapter has the following sections:

Overview of Certificate Management System

Certificate Management System is a highly configurable set of software components and tools for creating, deploying, and managing certificates. The standards and services that facilitate the use of public-key cryptography and X.509 version 3 certificates in a networked environment are collectively called the *public key infrastructure (PKI)* for that environment. In any PKI, a *certificate authority (CA)* is a trusted entity that issues, renews, and revokes certificates. An *end entity* is a person, router, server, or other entity that uses a certificate to identify itself.

To participate in a PKI, an end entity must *enroll*, or register, in the system. The end entity typically initiates enrollment by giving the CA some form of identification and a newly generated public key. The CA uses the information provided to *authenticate*, or confirm, the identity; it then issues the end entity a certificate that associates that identity with the public key, and signs the certificate with the CA's own private signing key.

End entities and CAs may be in different geographic or organizational areas or in completely different organizations. CAs may include third parties that provide services through the Internet as well as the root CAs and subordinate CAs for individual organizations. Policies and certificate content may vary from one organization to another. End-entity enrollment for some certificates may require physical verification, such as an interview or notarized documents, while enrollment for others may be fully automated.

To meet the widest possible range of configuration requirements, Certificate Management System permits the independent installation of four separate subsystems, or “managers,” that typically play distinct roles:

- **Certificate Manager**—A Certificate Manager functions as a root or subordinate certificate authority. This subsystem issues, renews, and revokes certificates, generates certificate revocation lists (CRLs). It can publish certificates to a Lightweight Directory Access Protocol (LDAP) directory and files, and CRLs to an LDAP directory, a file, and an Online Certificate Status Protocol (OCSP) responder. The Certificate Manager can be configured to accept requests from end entities, Registration Managers, or both, and can process requests either manually (that is, with the aid of a human being) or automatically (based entirely on customizable policies and procedures). When set up to work with a separate Registration Manager, the Certificate Manager processes requests and returns the signed certificates to the Registration Manager for distribution to the end entities. (For an overview of the role of certificate authorities and related concepts of public-key cryptography, see Appendix D of *Managing Servers with iPlanet Console*.)

  Note that the publishing tasks can be performed by the Certificate Manager only. The Certificate Manager also has a built-in OCSP service, enabling OCSP-compliant clients to directly query the Certificate Manager about the revocation status of a certificate that it has issued. In certain PKI deployments, it might be convenient to use the Certificate Manager’s built-in OCSP service, instead of a Online Certificate Status Manager.

- **Registration Manager**—A Registration Manager is an optional component in the PKI and can be used to separate the registration process from the certificate-signing process. The Registration Manager performs a subset of the end-entity tasks performed by the Certificate Manager, such as enrollment or renewal, on behalf of the Certificate Manager. A Registration Manager is typically installed on a different machine from the Certificate Manager that it serves. After the Registration Manager approves requests, it forwards them to this Certificate Manager, which trusts the Registration Manager to provide reliable authentication services and therefore trusts any signed requests it submits. The Certificate Manager processes the requests and issues the certificates. The Registration Manager then distributes the certificates to the end entities.

- **Data Recovery Manager**—A Data Recovery Manager oversees the long-term archival and recovery of private encryption keys for end entities. A Certificate Manager or Registration Manager can be configured to archive end entities' private encryption keys with a Data Recovery Manager as part of the process of issuing new certificates. The Data Recovery Manager is useful only if end entities are encrypting data (using applications such as S/MIME email) that the organization may need to recover someday. It can be used only with client software that supports dual key pairs—that is, two separate key pairs, one for encryption and one for digital signatures. This service is available in newer clients only; for example, Communicator versions 4.7x (with Netscape Personal Security Manager installed) and Netscape 6 support generation of dual key pairs. The Data Recovery Manager archives encryption keys. It does not archive signing keys, since such archival would undermine nonrepudiation properties of dual-key certificates.
- **Online Certificate Status Manager**—A Online Certificate Status Manager performs the task of an online certificate validation authority, by enabling OCSP-compliant clients to do real-time verification of certificates. The Online Certificate Status Manager can receive CRLs from multiple Certificate Managers and clients can query the Online Certificate Status Manager for the revocation status of certificates issued by all these Certificate Managers. For example, in a PKI comprising multiple CAs (a root CA and many subordinate CAs) each CA can be configured to publish its CRL to the Online Certificate Status Manager. This way, all clients in the PKI deployment can verify the revocation status of a certificate by querying the Online Certificate Status Manager.

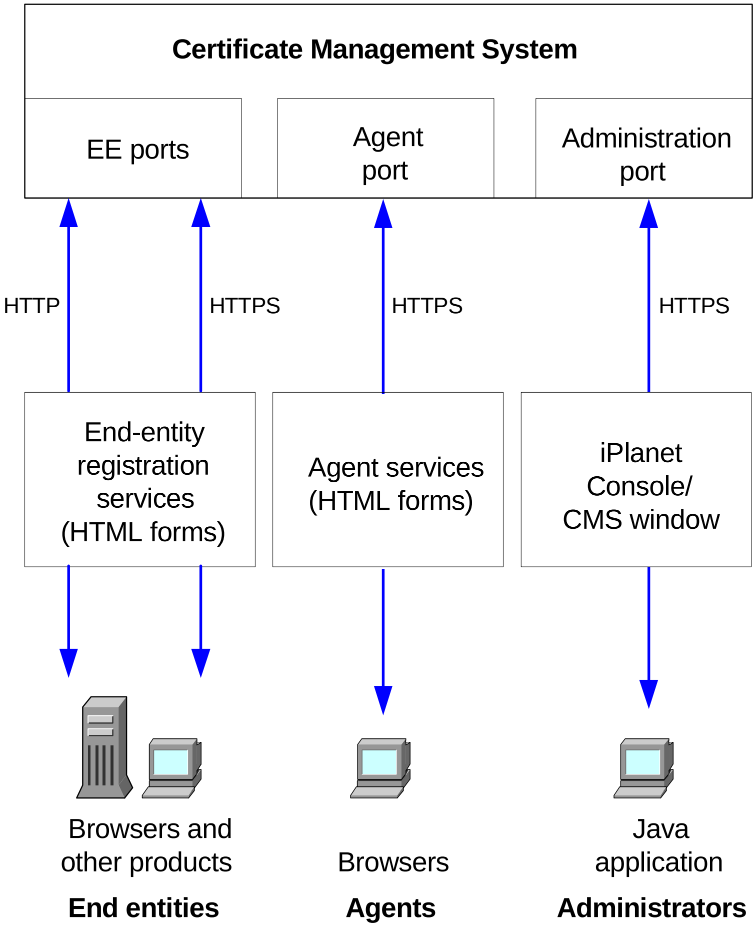
  Note that an online certificate-validation authority is often referred to as *OCSP responder*.

Since CAs can delegate some responsibilities to subordinate CAs, a Certificate Manager might delegate responsibilities to one or more levels of subordinate Certificate Managers, and Registration Managers might delegate responsibilities to subordinate Registration Managers. Therefore many complex variations are possible.

Three kinds of entities can access CMS subsystems: administrators, agents, and end entities. Administrators are responsible for the initial setup and ongoing maintenance of the subsystems. Administrators can designate users with special privileges, called agents, for each subsystem. Agents manage day-to-day interactions with end entities and other aspects of the PKI. This guide describes the tasks that agents can perform. End entities access Registration Manager or Certificate Manager subsystems to enroll in a PKI and to take part in other life-cycle management operations, such as renewal or revocation.

Figure 1-1 shows the ports used by administrators, agents, and end entities. All agent and administrator interactions with CMS subsystems occur over HTTPS. End-entity interactions can take place over HTTP or HTTPS.

Figure 1-1 Certificate Management System and its users


Certificate Management System
EE ports
Agent port
Administration port
HTTP
HTTPS
HTTPS
HTTPS
End-entity registration services (HTML forms)
Agent services (HTML forms)
iPlanet Console/ CMS window
Browsers and other products
Browsers
Java application
End entities
Agents
Administrators

Agent Tasks

The designated agents for each subsystem are responsible for the everyday management of end-entity requests and other aspects of the PKI:

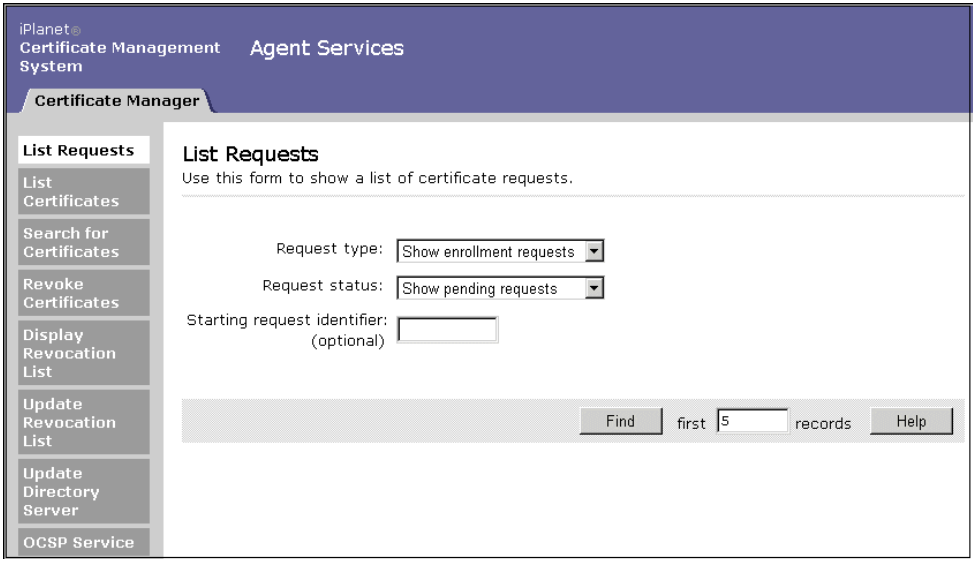
- Certificate Manager agents manage certificate requests received by the Certificate Manager subsystem, maintain and revoke certificates as necessary, and maintain global information about certificates.
- Registration Manager agents manage the certificate requests received by the Registration Manager subsystem.
- Data Recovery Manager agents initiate the recovery of lost keys, and can obtain information about key service requests and archived keys.
- Online Certificate Status Manager agents can perform tasks such as checking which CAs are currently configured to publish their CRLs to the Online Certificate Status Manager, identifying a Certificate Manager to the Online Certificate Status Manager, adding CRLs directly to the Online Certificate Status Manager, and viewing the status of OCSP service requests submitted by OCSP-compliant clients.

To perform the privileged operations of an agent, you use the CMS Agent Services pages. To access these pages, you must have a personal SSL client certificate, and the CMS administrator must have identified you as a privileged user in the user database. For more information on how to get set up as a privileged user, see *CMS Installation and Setup Guide*.

Certificate Manager Agent Services

The default entry page to the Certificate Manager agent services is shown in Figure 1-2. To access these pages, you must be a designated Certificate Manager agent and your client software must have a valid certificate identifying you as such.

Figure 1-2 Certificate Manager Agent Services page



List Requests

Use this form to show a list of certificate requests.

Request type: Show enrollment requests

Request status: Show pending requests

Starting request identifier: (optional)

first 5 records

As a Certificate Manager agent, you can perform the following tasks:

- Handle certificate requests.

  You can list the certificate service requests received by the Certificate Manager subsystem, assign requests to yourself, reject or cancel requests, and approve requests for certificate enrollment. See , “Handling Certificate Requests.”

- Clone requests.

  You can clone any request, whether it’s still pending, canceled, rejected, or completed. This can be useful in a variety of situations. For example, if a user receives a certificate that doesn’t work because it has been incorrectly formulated, you can locate the completed request, clone it, and correct it without requiring the user to enroll a second time. Cloning a request gives it a new request ID number and puts it into the list of pending requests, but does not change the status of the original request.

- Find certificates.

  You can search for individual certificates, or search for and list certificates by various criteria, then display the details of certificates you have found. See Chapter 3, “Finding and Revoking Certificates”

- Revoke certificates.

  If a user's key has been compromised, you need to revoke the user's certificate to ensure that the key is not misused. You may also need to revoke the certificates of users who have left the organization. You can use Certificate Manager Agent Services to find and revoke a specific certificate or a set of certificates. Users can also revoke their own certificates. See "Revoking Certificates" on page 53.

- Update the CRL.

  The Certificate Manager maintains a public list of certificates that have been revoked, called the certificate revocation list (CRL). The list is usually maintained automatically, but you may sometimes need to use the Certificate Manager Agent Services page to update the list manually. See "Updating the CRL" on page 58.

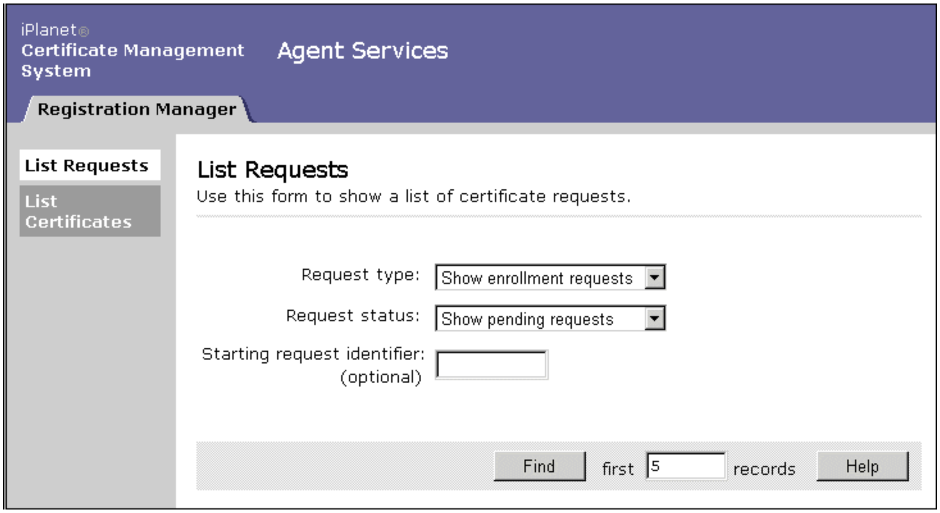
- Publish certificates to a directory.

  You can set up Certificate Management System to publish certificates and lists of revoked certificates in an LDAP directory. Certificate information is usually published automatically, but you may sometimes need to use the Certificate Manager Agent Services page to update the directory manually. See Chapter 4, "Publishing to a Directory"

Registration Manager Agent Services

The default entry page to the Registration Manager agent services is shown in Figure 1-3. To access these pages, you must be a designated Registration Manager agent and your client software must have a valid certificate identifying you as such.

Figure 1-3 Registration Manager Agent Services page



List Requests

Use this form to show a list of certificate requests.

Request type: Show enrollment requests

Request status: Show pending requests

Starting request identifier: (optional)

first 5 records

As a Registration Manager agent, you can perform the following tasks:

- Handle certificate requests.

  You can list the certificate service requests received by the Registration Manager subsystem, assign requests to yourself, reject or cancel requests, clone requests, and approve enrollment requests to be passed on to the Certificate Manager for issuance. See Chapter 2, “Handling Certificate Requests”

- Find certificates.

  You can search for individual certificates, or search for and list certificates by various criteria, then display the details of certificates you have found. See Chapter 3, “Finding and Revoking Certificates”

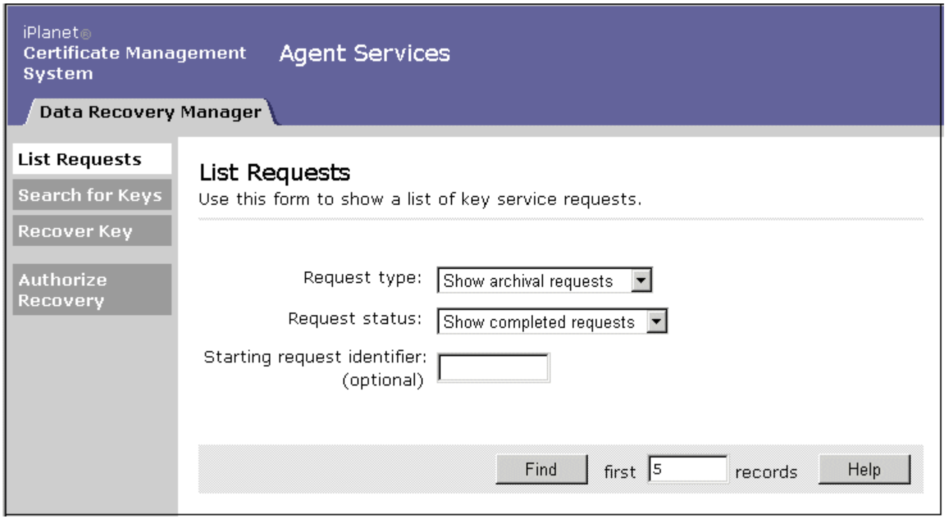
- Revoke certificates.

  If a user’s key has been compromised, you need to revoke the user's certificate to ensure that the key is not misused. You may also need to revoke the certificates of users who have left the organization. You can use Registration Manager Agent Services to find and revoke a specific certificate or a set of certificates. Users can also revoke their own certificates. See “Revoking Certificates” on page 53.

Data Recovery Manager Agent Services

The default entry page to the Data Recovery Manager agent services is shown in Figure 1-4. To access these pages, you must be a designated Data Recovery Manager agent and your client software must have a valid certificate identifying you as such.

Figure 1-4 Data Recovery Manager Agent Services page



List Requests

Use this form to show a list of key service requests.

Request type: Show archival requests

Request status: Show completed requests

Starting request identifier: (optional)

first 5 records

As a Data Recovery Manager agent, you can perform the following tasks:

- List key recovery requests from end entities.
- List or search for archived keys.
- Initiate the recovery of private data-encryption keys.

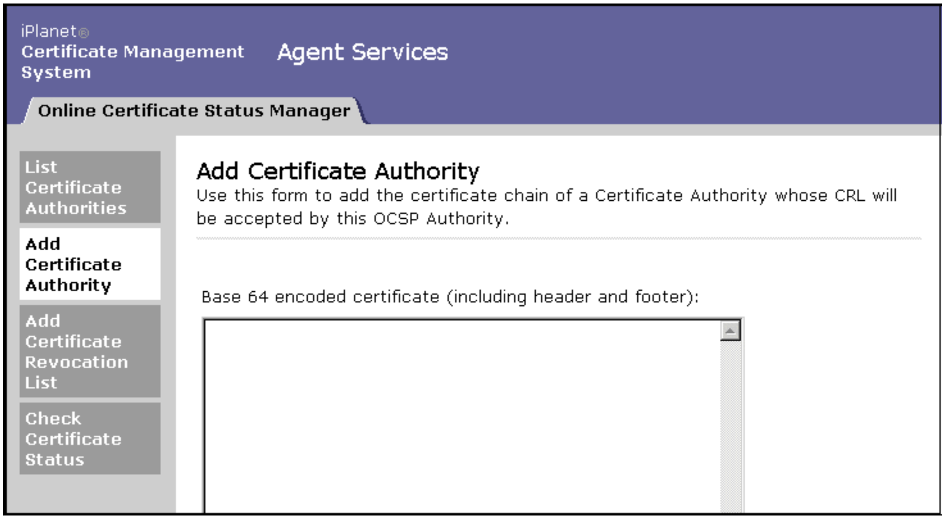
Key recovery requires the authorization of one or more *recovery agents.* The administrator for the Data Recovery Manager designates recovery agents. Typically, several recovery agents own portions of the storage key for the Data Recovery Manager. The approval of *m* of a total of *n* agents is required to authorize key recovery. The values of *m* and *n* for your installation of the Data Recovery Manager is determined by the administrator in charge of the subsystem.

For more information on these tasks, see Chapter 5, "Recovering Encrypted Data."

Online Certificate Status Manager Agent Services

The default entry page to the Online Certificate Status Manager agent services is shown in Figure 1-5. To access these pages, you must be a designated Online Certificate Status Manager agent and your client software must have a valid certificate identifying you as such.

Figure 1-5 Online Certificate Status Manager Agent Services page



iPlanet®
Certificate Management System
Agent Services
Online Certificate Status Manager
List Certificate Authorities
Add Certificate Authority
Add Certificate Revocation List
Check Certificate Status

Add Certificate Authority

Use this form to add the certificate chain of a Certificate Authority whose CRL will be accepted by this OCSP Authority.

Base 64 encoded certificate (including header and footer):

As a Online Certificate Status Manager agent, you can perform the following tasks:

- Checking which CAs are currently configured to publish their CRLs to the Online Certificate Status Manager.
- Identifying a Certificate Manager to the Online Certificate Status Manager.
- Adding CRLs directly to the Online Certificate Status Manager.
- Checking the revocation status of a certificate by submitting it to the Online Certificate Status Manager.

For more information on these tasks, see Chapter 6, “Managing OCSP Service Related Tasks.”

Forms for Performing Agent Operations

The agent services consist of a form-based HTML interface that is part of your Certificate Management System installation. The CMS administrator designates particular users as agents for each installed subsystem (Certificate Manager, Registration Manager, Data Recovery Manager, and). Only a designated agent for a subsystem can use the Agent Services interface for that subsystem. In addition, you must have a personal client SSL certificate to access the Agent Services interface.

As a subsystem agent with the proper certificate, you use the Agent Services page to access the forms you need to perform the agent tasks. Table 1-1 describes each of these HTML forms.

Table 1-1 Forms used for agent operations

Form name	Description
List Requests (Certificate Manager and Registration Manager)	Use this form to examine, select, and process requests for certificate services. Both Certificate Manager and Registration Manager agents can use this form. For instructions on using this form, see “Listing Certificate Requests” on page 32 in Chapter 2.
List Certificates (Certificate Manager)	Use this form to list certificates within a range of serial numbers. You can limit the list to valid certificates. Only Certificate Manager agents can use this form. For instructions on using this form, see “Basic Certificate Listing” on page 45 in Chapter 3.
Search for Certificates (Certificate Manager)	Use this form to search for and list certificates issued by Certificate Management System. Only Certificate Manager agents can use this form. This form allows you to search by subject name or by certificate type, the state of the certificate (expired, revoked, and so on), and the dates when the certificate was issued or revoked, expired, or became valid. For instructions on using this form, see“Advanced Certificate Search” on page 47 in Chapter 3.
Revoke Certificates (Certificate Manager)	Use this form to search for and revoke certificates issued by Certificate Management System. Only Certificate Manager agents can use this form. For instructions on using this form, see “Revoking Certificates” on page 53 in Chapter 3.

Table 1-1 Forms used for agent operations *(Continued)*

Form name	Description
Update Revocation List (Certificate Manager)	Use this form to manually update the published list of revoked certificates. Only Certificate Manager agents can use this form. For instructions on using this form, see "Managing the Certificate Revocation List" on page 57 in Chapter 3.
Update Directory Server (Certificate Manager)	Use this form to update the LDAP publishing directory with changes in certificate information (newly issued certificates, updated CRLs, and so on). Only Certificate Manager agents can use this form. For instructions on using this form, see"Updating the Directory with Changes" on page 62 in Chapter 4.
List Requests (Data Recovery Manager)	Use this form to find and examine requests for key services. Only Data Recovery Manager agents can use this form. For instructions on using this form, see"Viewing Key Service Requests" on page 72 in Chapter 5.
Search for Keys (Data Recovery Manager)	Use this form to find and list specific archived keys. Only Data Recovery Manager agents can use this form. For instructions on using this form, see "Finding Archived Keys" on page 66 in Chapter 5.
Recover Keys (Data Recovery Manager)	Use this form to find and recover specific archived keys. Only Data Recovery Manager agents can use this form. You can select a key in the list returned by a search and initiate its recovery, which must be authorized by designated key recovery agents. For instructions on using this form, see "Recovering Keys" on page 69 in Chapter 5.
Authorize Recovery (Data Recovery Manager)	Use this form to remotely authorize a key recovery request initiated by another Data Recovery Manager agent. Key recovery agents do not have to be Data Recovery Manager agents if key recovery is handled locally; however, only key recovery agents who are also Data Recovery Manager agents can access this form. For instructions on using this form, see "Recovering Keys" on page 69 in Chapter 5.
List Certificate Authorities (Online Certificate Status Manager)	Use this form to list Certificate Managers that are currently configured to publish their CRLs to the Online Certificate Status Manager. For instructions, see "Listing CAs Identified by Online Certificate Status Manager" on page 77 in Chapter 6.

Table 1-1 Forms used for agent operations *(Continued)*

Form name	Description
Add Certificate Authority (Online Certificate Status Manager)	Use this form to identify a Certificate Manager to the Online Certificate Status Manager. For instructions, see "Identifying a CA to Online Certificate Status Manager" on page 78 in Chapter 6.
Add Certificate Revocation List (Online Certificate Status Manager)	Use this form to add a CRL to the Online Certificate Status Manager's internal database. For instructions, see "Adding a CRL to Online Certificate Status Manager" on page 80 in Chapter 6.
Check Certificate Status (Online Certificate Status Manager)	Use this form to check the status of OCSP service requests sent by OCSP-compliant clients. For instructions, see "Checking the Revocation Status of a Certificate" on page 82 in Chapter 6.

Accessing Agent Services

Access to the agent services forms requires certificate-based authentication. Only users who authenticate with the correct certificate and who have been granted the proper access privilege can access and use the forms. The operation uses the SSL protocol; that is, you connect to the server using HTTPS (not HTTP) on the SSL agent port. For example, if Certificate Management System is installed on a host named `cert.siroe.com` and is running on port 443 (the default port for SSL connections), you invoke the Agent Services interface by using the following URL:

```
https://cert.siroe.com:443
```

The Agent Services pages are written in HTML and are intended to be customized. This document describes the default pages. If your administrator has customized these pages, yours may differ from those described here. Check with the CMS administrator for information on your local installation.

Administrator/Agent Certificate Enrollment

Immediately after installing any CMS instance, the administrator must enroll for the initial administrator/agent certificate. This is the first user certificate that Certificate Management System issues.

The initial user is both an administrator and an agent. This person can create additional agents with the appropriate user privileges and issue them certificates. Since there is no agent yet to approve the request, a special enrollment form allows you to get this first certificate automatically.

After you submit this initial Administrator / Agent Certificate Enrollment form, it is automatically disabled, so that no one else can acquire a certificate without agent approval or some form of automated authentication. The system automatically adds the initial user to the list of agents.

To enroll for the first agent certificate, you should be working at the computer you intend to use as the agent, so that the new certificate will be installed in the browser you will be using to access the Agent Services pages. Follow these steps:

1. Open a web browser window.

2. Go to the URL for the SSL agent port.

   By default, this is a URL of the following form:

   `https://<hostname>:<agent_port>`

   `<hostname>` is the fully qualified domain name of the machine on which Certificate Management System is installed; for example, `cert.siroe.com`.

   `<agent_port>` is the TCP port specified during installation for agent communications over SSL; for example, 8100.

   The first time you access this port, the system opens the Administrator / Agent Certificate Enrollment form.

   Because you have accessed an SSL port, Certificate Management System presents its server SSL certificate to your browser for authentication. This is the server SSL certificate that you created during installation. Because you just created it, it is not on your browser's list of trusted certificates. Before you see the Administrator / Agent Certificate Enrollment form, a series of dialog boxes appear that let you add the CMS server certificate to your list of trusted certificates.

3. Complete the dialog boxes as instructed (the exact procedure depends on the browser you are using).

4. In the Administrator / Agent Certificate Enrollment form, enroll for a client SSL certificate as the system's first privileged user by entering the following information:

   Authentication Information section:

   User ID. The ID you entered for the CMS administrator during installation.

Password. The password you specified for the CMS administrator during installation.

Subject Name section (The subject name is the distinguished name (DN) that identifies the certified owner of the certificate.)

Full name. Name of administrator/agent.

Login name. User ID of administrator/agent.

Email address. Email address of administrator/agent.

Organization unit. Name of the organization unit to which the administrator/agent belongs.

Organization. Name of the company or organization the administrator/agent works for.

Country. Two-letter code for the administrator/agent's country.

User's Key Length Information section:

Key Length. The length of the private key that will be generated by your browser. This key corresponds to the public key that is part of the administrator/agent certificate.

Note that the validity period of this initial agent certificate is hard-coded as one year.

5. Click Submit.
6. Follow the instructions your browser presents as it generates a key pair.
7. If authentication is successful, the new certificate will be imported into your browser, and you will be given an opportunity to make a backup copy.

Now you have a client authentication certificate in the name you specified. This special user, who was named as the initial administrator for Certificate Management System during installation, has been automatically designated as the first agent. This certificate allows you to access the Agent Services pages. As an agent, you can approve enrollment requests and start issuing new certificates. To access the CMS windows in iPlanet Console, you use the user ID that you specified for the certificate and the corresponding password—both of which must correspond to the values you specified for the CMS administrator during installation.

Note that after you submit the initial Administrative Enrollment form, it is no longer available from the agent port. If something goes wrong and you are unable to obtain the administrator/agent certificate, you must reset a parameter in the configuration file to make the initial administrative enrollment form available again. Follow these steps:

1. In the left frame of iPlanet Console, open the CMS instance for which you want to display the Administrator/Agent Certificate Enrollment form.

   The server requests the password for the CMS administrator.

2. Click the icon labeled “Stop the Server.”
3. Go to this directory: `<server_root>/cert-<instance_ID>/config`
4. Open the `CMS.cfg` file in a text editor, and find the following line: `agentGateway.enableAdminEnroll=false`
5. Change `false` to `true`, and save the file.
6. Start the server from the CMS window where you stopped it. (Alternatively, right-click on the name of the instance in the left frame and choose Start Server.) At this point, the server asks you for the single signon password you specified during installation.
7. The next time you access the SSL agent port, the Administrator/Agent Certificate Enrollment form will be available again.

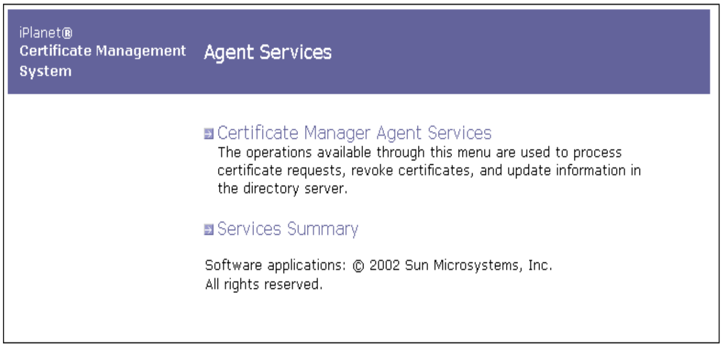
Agent Services Entry Page

To access the Agent Services interface in a default installation:

1. Open a browser.
2. Go to the URL for the SSL agent port.

   This is the same URL you used to access the initial Administrator/Agent Certificate Enrollment form.

3. In the Agent Services entry page, click the subsystem whose agent services you require.



iPlanet®
Certificate Management System
Agent Services

Certificate Manager Agent Services
The operations available through this menu are used to process certificate requests, revoke certificates, and update information in the directory server.

Services Summary

Software applications: © 2002 Sun Microsystems, Inc.
All rights reserved.

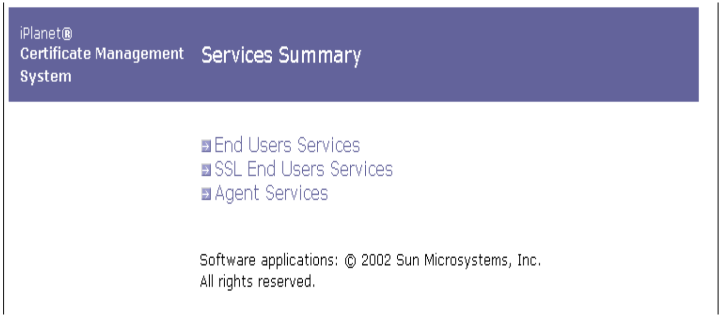
The choices depend on which subsystems have been installed in the particular Certificate Management System instance. If you present a valid certificate and have been designated as an agent for a subsystem, you can access and use the Agent Services pages for that subsystem by clicking the link on this page.

If you do not yet have your certificate, click Services Summary to enroll for one. For more information, see “Services Summary Page” (the next section).

Services Summary Page

If you want to access another gateway without looking up the port number, click Services Summary on the Agent Services entry page. The Services Summary page gives you access to each of the configured gateways: the HTTPS end-entity gateway, the HTTP end-entity gateway (if it has been enabled), and the Agent Services entry page.

Figure 1-6 Services Summary page



iPlanet®
Certificate Management System
Services Summary

End Users Services
SSL End Users Services
Agent Services

Software applications: © 2002 Sun Microsystems, Inc.
All rights reserved.

If you do not yet have a certificate that allows you access to the Agent Services pages, go to one of the end-entity gateways and enroll for your certificate.

Chapter 2

Handling Certificate Requests

As a Certificate Manager or Registration Manager agent, you are responsible for handling both manual enrollment requests made by end entities (end users, server administrators, or other CMS subsystems) and automated enrollment requests that have been deferred. This chapter describes the general procedure for handling requests and explains how to handle different aspects of certificate request management.

The chapter has the following sections:

- Managing Requests (page 29)
- Listing Certificate Requests (page 32)
- Approving Requests (page 36)
- Other Options for Handling Requests (page 43)

Managing Requests

This the typical procedure for handling certificate enrollment requests:

1. View the list of pending requests for the Certificate Manager or Registration Manager (see "Listing Certificate Requests" on page 32).
2. Select a request from the list to view it and, optionally, assign the request to yourself (see "Selecting a Request" on page 35).

3. Process the request (see "Approving Requests" on page 36 and "Other Options for Handling Requests" on page 43).

   In processing a request for a certificate, you can choose to take one of the following actions:

   - **Approve the request.** You can approve a request manually, or it can be approved automatically by policy modules if the request has been authenticated by an authentication module (and if the CMS administrator has configured the system to do this). After a request has been approved, Certificate Management System issues the requested certificate (Certificate Manager) or passes it on to the Certificate Manager for issuance (Registration Manager).

   - **Reject the request.** You can reject a request manually, or it can be rejected automatically by a policy module if it does not conform to your organization's policies. If the CMS administrator has configured the system to provide automatic notifications to end users, a rejected request will automatically result in such a notification being sent.

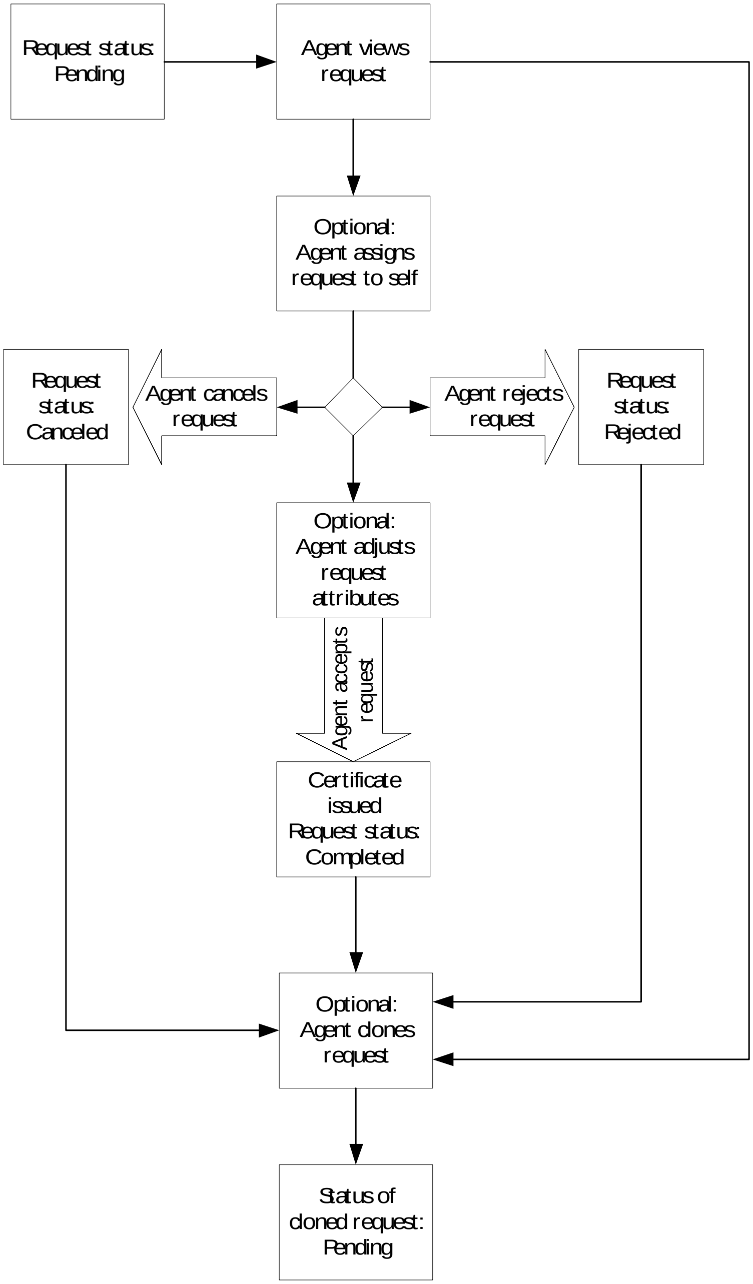
   - **Cancel the request.** You can cancel a request manually, but requests are never cancelled automatically, and users do not receive automatic notification of cancelled requests. Cancellation can be useful, for example, if the user has left the company since submitting the request, or if you have already talked to the user over the phone about the problem and therefore don't need to invoke automatic notification.

   Each of these actions changes the status of the certificate request. If you close the form without taking one of these actions, the request remains in the queue with the same status.

   It's also possible to clone any request, whether it's still pending, canceled, rejected, or completed. This can be useful in a variety of situations. For example, if a user receives a certificate that doesn't work because it has been incorrectly formulated, you can locate the completed request, clone it, and correct it without requiring the user to enroll a second time. Cloning a request gives it a new request ID number and puts it into the list of pending requests, but does not change the status of the original request.

   Figure 2-1 illustrates the process for handling requests and the different types of status for a request.

Figure 2-1 The certificate request management process


Request status: Pending
Agent views request
Optional: Agent assigns request to self
Request status: Canceled
Agent cancels request
Agent rejects request
Request status: Rejected
Optional: Agent adjusts request attributes
Agent accepts request
Certificate issued Request status: Completed
Optional: Agent clones request
Status of cloned request: Pending

Listing Certificate Requests

The Certificate Manager or Registration Manager keeps a queue of all certificate service requests that have been submitted to it. The queue records whether a request is pending, completed, canceled, or rejected. Four types of requests can be in the queue:

- Enrollment requests
- Revocation requests
- Renewal requests
- Certificate chain requests

As a Certificate Manager or Registration Manager agent, you must review and approve manual enrollment requests; those that require review have a status of Pending.

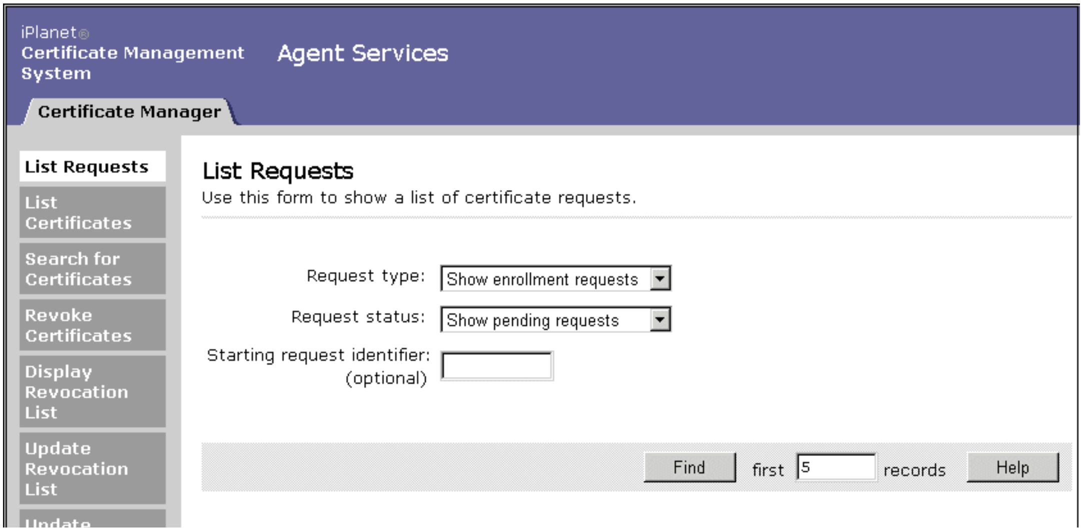
To see a list of requests:

1. Go to the Registration Manager or Registration Manager Agent Services page (see “Accessing Agent Services” on page 23).

   You must submit the proper client certificate to get access to this page.

2. Click List Requests at the top of the left frame to view the queue of requests for certificates and to issue those certificates.

   The List Requests form appears.



List Requests

Use this form to show a list of certificate requests.

Request type: Show enrollment requests

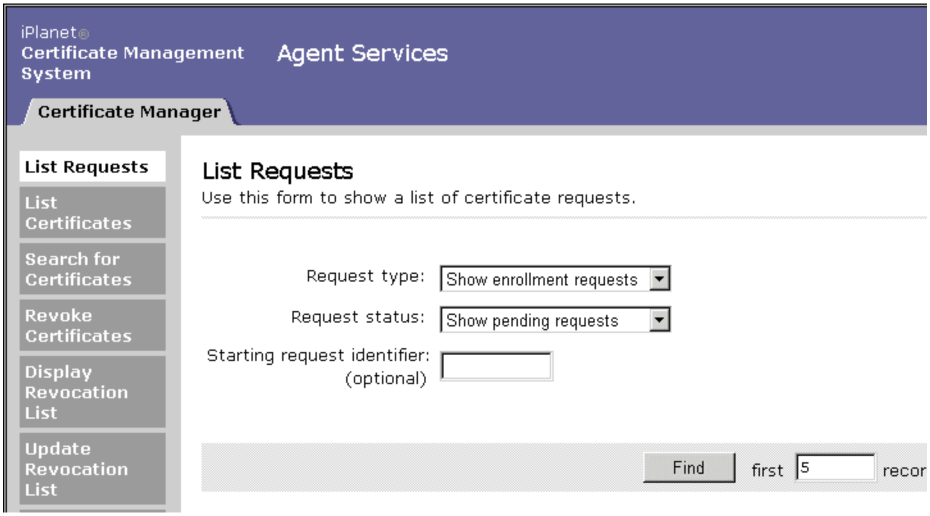
Request status: Show pending requests

Starting request identifier: (optional)

first 5 records

3. Choose the type of requests you want to see by selecting one of the following from the "Request type" menu:

   - **Show enrollment requests**
   - **Show renewal requests**
   - **Show revocation requests**
   - **Show all requests**



List Requests

Use this form to show a list of certificate requests.

Request type: Show enrollment requests

Request status: Show pending requests

Starting request identifier: (optional)

Find first 5 recor

4. Choose the status of requests you want to see by selecting one of the following from the "Request status" menu:

   - **Show pending requests**

     These are enrollment requests that have not yet been processed but are waiting for manual review. Requests in this state may already be assigned to an issuing agent for processing.

   - **Show canceled requests**

     These are requests that have been manually canceled by an agent. Users do not receive automatic notification of canceled requests. Cancellation can be useful, for example, if the user has left the company since submitting the request, or if you have already talked to the user over the phone about the problem and therefore don't need to invoke automatic notification.

- **Show rejected requests**

  These are requests that have been either manually rejected or rejected automatically during policy processing. If the CMS administrator has configured the system to provide automatic notifications to users, a rejected request will automatically result in such a notification being sent.

- **Show completed requests**

  These are requests that have been completed. They include enrollment requests for which certificates have been issued and also completed revocation and certificate chain requests.

- **Show all requests**

  This will show all requests of the selected type, regardless of status.

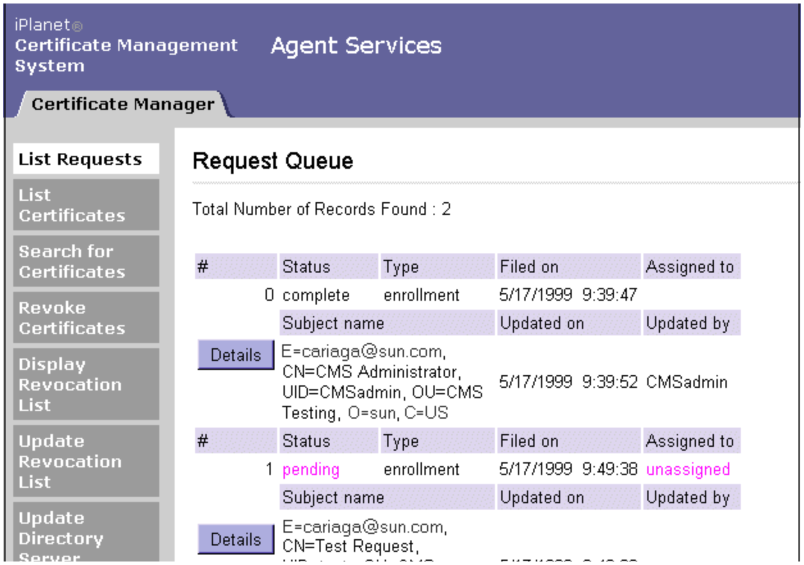
5. To start the list at a specific place in the queue, enter the starting request identifier in decimal or hexadecimal form.

   Use `0x` to indicate a hexadecimal number; for example, `0x2A`.

6. Choose the number of matching requests you want to see. When you specify a number *n*, the system displays the first *n* requests after the starting sequence number that matches your specified criteria.

7. Click Find to display the list of requests that match your specified criteria.

   The Request Queue form appears.



Request Queue

Total Number of Records Found : 2

#	Status	Type	Filed on	Assigned to
0	complete	enrollment	5/17/1999 9:39:47	
	Subject name		Updated on	Updated by
Details	E=cariaga@sun.com, CN=CMS Administrator, UID=CMSadmin, OU=CMS Testing, O=sun, C=US		5/17/1999 9:39:52	CMSadmin
#	Status	Type	Filed on	Assigned to
1	pending	enrollment	5/17/1999 9:49:38	unassigned
	Subject name		Updated on	Updated by
Details	E=cariaga@sun.com, CN=Test Request,			

Selecting a Request

To select a request from the queue:

1. On the Agent Services page, click List Requests, specify search criteria, and click Find to display a list of certificate signing requests.

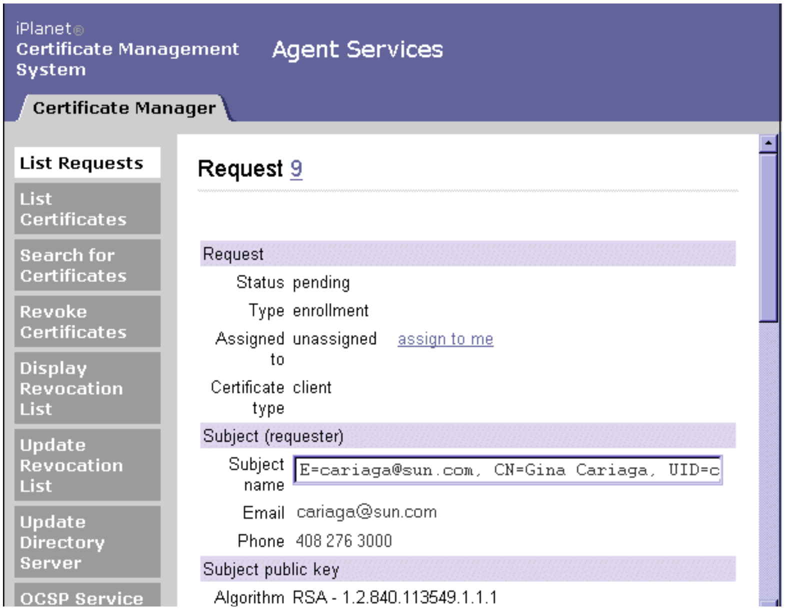
   See "Listing Certificate Requests" on page 32 for details.

2. On the Request Queue form, find the particular request you want to examine.

   If the request you want to see is not shown, scroll to the bottom of the list, specify an additional number *n*, and click Find. The system displays the next *n* requests that match your original search criteria.

3. When you have found the request you want, click Details at the left.

   The Request details form appears, showing detailed information about the selected request. Use this form to approve or otherwise handle the request. For more information, see "Approving Requests" on page 36 and "Other Options for Handling Requests" on page 43.



Request 9

Request

Status pending

Type enrollment

Assigned to unassigned assign to me

Certificate type client

Subject (requester)

Subject name E=cariaga@sun.com, CN=Gina Cariaga, UID=c

Email cariaga@sun.com

Phone 408 276 3000

Subject public key

Algorithm RSA - 1.2.840.113549.1.1.1

If the system changes the state of the displayed request, and if you use your browser's Back or Forward buttons or the Go (history) menu to move to another page, the data shown can become out of date. To refresh the data, click the highlighted serial number at the top of the page.

Approving Requests

As an agent, you can approve a certificate request. If the request was made directly to the Certificate Manager, it issues the certificate; if the request was made through a Registration Manager, the Registration Manager passes the approved request on to the Certificate Manager for issuance. Before approving a request, you can assign it to yourself, adjust the attributes of the request, and verify that it will result in a valid certificate. To do these things, use the Request Details form that appears when you examine a selected request (as described in "Selecting a Request" on page 35). If you want to reject or cancel the request, see "Other Options for Handling Requests" on page 43.

The approval and issuing process has the following stages:

- Assigning a Request
- Adjusting, Verifying, and Approving a Request
- Sending an Issued Certificate to the Requester

Assigning a Request

Before acting on a request, you can assign it to yourself. Assignment is not required; any agent can act on an unassigned request. When a request is assigned to a particular agent, all agents can examine that request, but only the assigned agent can act on it. When a request is assigned to another agent, however, you can choose to reassign it to yourself in order to act on it.

When you view the details of an unassigned request, you can click "assign to me" to assign it to yourself. The request is immediately assigned to you, and the Request Details page reflects the assignment. If you leave the page without approving, rejecting, or canceling the request, the request remains in the queue with the status of Pending, but it is assigned to you.

Adjusting, Verifying, and Approving a Request

Before you verify and approve a request, you can adjust some of the parameters, such as the subject name and validity period.

To adjust, verify, and approve a certificate request:

1. Select the certificate request from a list of requests, as described in "Selecting a Request" on page 35.

2. In the Service Request form, check the Assigned To prompt to see if the certificate request is assigned to you.

   ❍ If the request is unassigned, you can choose to assign it to yourself. Click "assign to me." Your CMS login name appears as the assigned agent, and the "assign to me" link changes to "cancel request assignment."

   ❍ If the request is already assigned to you, you can choose to cancel the assignment. To cancel the request's assignment, click "cancel request assignment." The form then shows that the request is unassigned. You can still act upon an unassigned request.

   ❍ If the request is assigned to another agent, you cannot act on the request unless you reassign it to yourself. Click "re-assign to me." Your CMS login name appears as the assigned agent, and the "re-assign to me" link changes to "cancel request assignment."

3. To change the subject name, enter a new value in the Subject Name field.

   For example, you might need to change the subject name to prevent duplications or to correct spelling errors. Nothing prevents you from issuing many different certificates with the same subject name. However, in current versions of Netscape software (Netscape Navigator, Netscape Communicator, and Netscape servers), you cannot install more than one certificate with a particular subject name.

4. If you want to change the validity period, you can set the dates directly using the menus for start and end times or you can select a predefined period from the "Length of validity period" menu. Making a selection from the "Length of validity period menu" sets the "Not valid after" date based on the "Not valid before date" and your selection.

5. Use the Extensions section to specify Netscape certificate type bits that you want to be set in the issued certificate.

   ❍ To specify the intended use of the certificate that you are issuing, select one or more types from the list of Netscape certificate types, as described below. If you select any of these types, the equivalent Netscape certificate type bit is set.

Table 2-1 Netscape certificate type extension

Type	Description
SSL client	Indicates that the certificate is a personal certificate used by Netscape Navigator to establish SSL connections with servers.

Table 2-1 Netscape certificate type extension *(Continued)*

Type	Description
SSL server	Indicates that the certificate is a server certificate used by a server to establish SSL connections with clients.
Secure Email	Indicates that the certificate is used by an email application to send and receive signed and encrypted email.
Object signing	Indicates that the certificate is used for object signing.
Subordinate SSL CA (available only for CA certificate requests)	Allows a CA to sign and issue personal and server certificates.
Subordinate email CA (available only for CA certificate requests)	Allows a CA to sign and issue certificates for use with signed and encrypted email.
Subordinate executable object-signing CA	Allows a CA to sign and issue object-signing certificates.

Note that additional extensions can be set by means of policy modules, which must be configured by the CMS administrator.

6. If you want to add extensions other than Netscape cert type extensions, you can paste a base-64 encoding of the extension in the “Additional Extensions” field.

   You can use the tools provided for generating extensions to include in CA and other certificate requests. For details about these tools, check this directory:

   ```
   <server_root>/bin/cert/tools
   ```

   The certificate extension text field accepts a single extension blob. If you want to add multiple extensions, you should use the ExtJoiner program, which is also provided in the above directory. For details about this tool, see “Extension Joiner Tool” in *CMS Command-Line Tools Guide*.

7. If you want the certificate to be signed using a signature algorithm other than the default, choose an alternative from the “Signature algorithm” drop-down list:

   - MD5 with RSA and MD2 with RSA generate a 128-bit message digest. Most existing software applications that handle certificates support only MD5. This is the default algorithm.

- SHA-1 with RSA generates a 160-bit message digest. Before choosing SHA-1, make sure your applications support it. Netscape Navigator 3.0 (or later) and Enterprise Server 2.01 (or later) support SHA-1. If your users have previous versions of these applications, choose MD5 as the signature algorithm, or upgrade your users to the most recent version of these applications.

Before selecting an algorithm, check with your CMS administrator to make sure that Certificate Management System has the algorithm enabled.

8. Review the unauthenticated request attributes. These attriubutes were submitted by the end entity with the enrollment request. Since these attributes do not come from a trusted source (such as an authentication module in the CMS server), they are “unauthenticated.” Your site policies may or may not require agents to review or validate any of these attributes.

9. Review the authenticated attributes. These attributes were generated in the CMS server by authentication or policy plug-in modules. They are considered authenticated since they have been validated by or have originated in the CMS server itself.

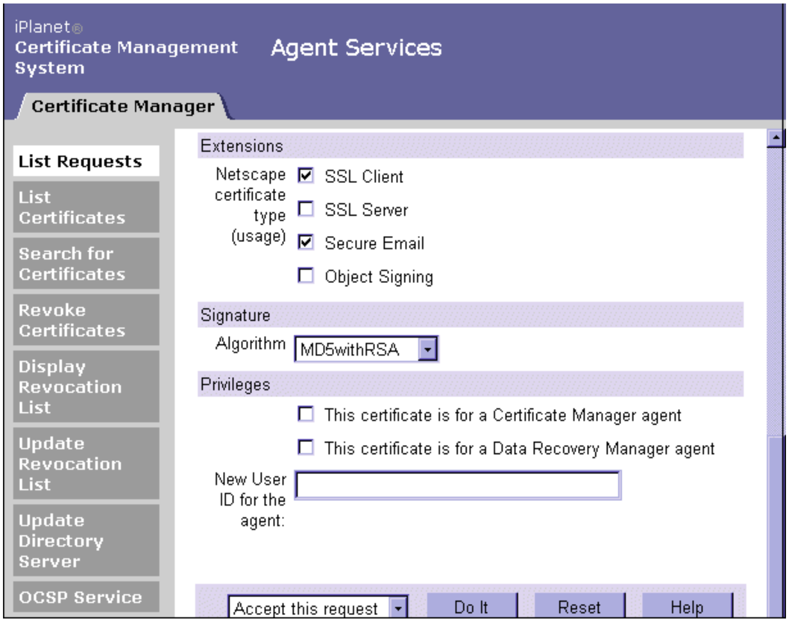
10. If the certificate request is for an SSL client certificate for a CMS manager or a CMS agent, you should indicate this in the last section, labeled Privileges.

    - If the request is for a CMS manager’s certificate, select the checkbox labeled “This certificate is for a Trusted Manager.”

    - If the request is for a CMS agent’s certificate, select the checkbox labeled “This certificate is for a *name of manager* agent.”

    You must also type a user ID for the new manager or agent. This user ID can be the same that you specified in the certificate request, or it can be some other ID that you want to use to identify this agent or manager in the CMS window of iPlanet Console, such as `Agent1` or `RMEng`.

11. To approve the request and issue the certificate, open the drop-down menu at the bottom of the page, choose "Accept this request," then click Do It.



Extensions

Netscape certificate type (usage)

☑ SSL Client

☐ SSL Server

☑ Secure Email

☐ Object Signing

Signature

Algorithm: MD5withRSA

Privileges

☐ This certificate is for a Certificate Manager agent

☐ This certificate is for a Data Recovery Manager agent

New User ID for the agent:

Accept this request

If the certificate conforms to policy, a page containing the new certificate appears. It includes instructions on how to help the certificate requester install the new certificate.

NOTE If, after verifying or attempting to issue the certificate, you receive the error message “The requested signature algorithm is not enabled,” check with your CMS administrator to make sure that the signature algorithm you selected in Step 7 is supported.

Sending an Issued Certificate to the Requester

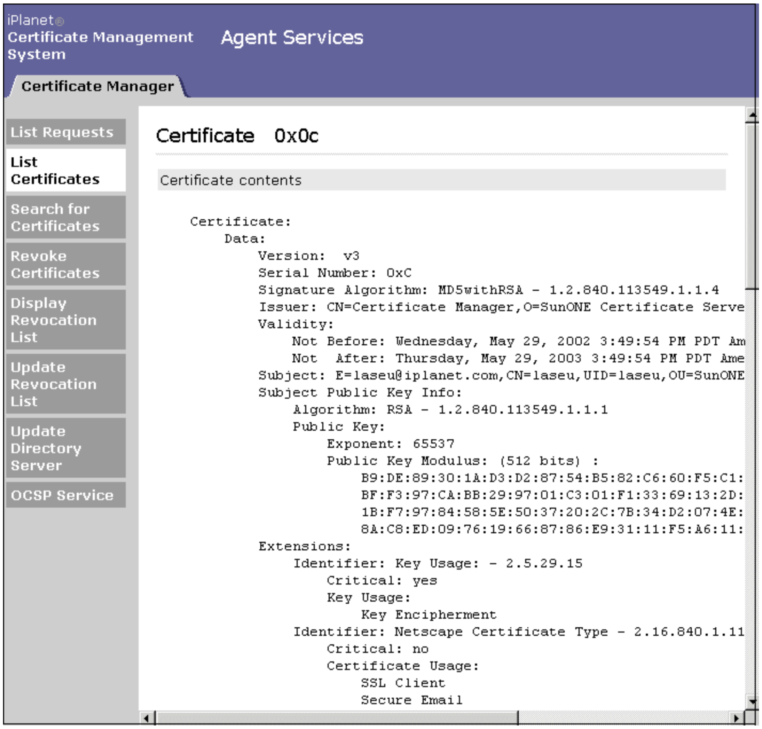
When the Certificate Manager has issued a certificate in response to a request, the user who requested it must receive a copy of it to install locally. End users install their own certificates in their client software. Server administrators install their servers’ certificates in the servers that they manage.

Depending on how your Certificate Management System is configured, an end user who requests a certificate might receive automatic email notification of the success of the request; this email message contains either the certificate itself or a URL from which the user can get the certificate. In this case, you need not take any further action.

If your system is not configured for automatic certificate-issuance notification, or if the requester is a server administrator, you must either send the issued certificate to the requester or ask the requester to pick it up from the Certificate Manager's end-entity gateway.

Figure 2-2 shows a web page containing a new certificate. This is the page you receive in response to the command "Issue this certificate," as described in Step 11 in "Approving Requests" on page 36.) Before you issue the certificate, you should copy the requester's email address.

Figure 2-2 A newly issued certificate page



Certificate 0x0c

Certificate contents

```
Certificate:
    Data:
        Version:  v3
        Serial Number: 0xC
        Signature Algorithm: MD5withRSA - 1.2.840.113549.1.1.4
        Issuer: CN=Certificate Manager,O=SunONE Certificate Serve
        Validity:
            Not Before: Wednesday, May 29, 2002 3:49:54 PM PDT Am
            Not  After: Thursday, May 29, 2003 3:49:54 PM PDT Ame
        Subject: E=laseu@iplanet.com,CN=laseu,UID=laseu,OU=SunONE
        Subject Public Key Info:
            Algorithm: RSA - 1.2.840.113549.1.1.1
            Public Key:
                Exponent: 65537
                Public Key Modulus: (512 bits) :
                    B9:DE:89:30:1A:D3:D2:87:54:B5:82:C6:60:F5:C1:
                    BF:F3:97:CA:BB:29:97:01:C3:01:F1:33:69:13:2D:
                    1B:F7:97:84:58:5E:50:37:20:2C:7B:34:D2:07:4E:
                    8A:C8:ED:09:76:19:66:87:86:E9:31:11:F5:A6:11:
        Extensions:
            Identifier: Key Usage: - 2.5.29.15
                Critical: yes
                Key Usage:
                    Key Encipherment
            Identifier: Netscape Certificate Type - 2.16.840.1.11
                Critical: no
                Certificate Usage:
                    SSL Client
                    Secure Email
```

To copy and mail a new server certificate to the requester, follow these steps:

1. Open a new email message composition window and address it to the requester.
2. From the Agent Services window where the new certificate is displayed, copy only the base-64 encoded certificate. Be sure to include the marker lines `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----`.
3. Paste the base-64 encoded certificate into the addressed email message and send the message.

To deliver a new client certificate to the requester, note the serial number of the request you approved, then follow these steps:

1. Go to the Agent Services gateway, click List Requests in the left frame, enter the serial number for the request that you approved, and click Find.
2. In the Request Queue form, click Details beside the relevant request, then right-click the certificate serial number and choose Open Frame in New Window from the pop-up menu.
3. In the new browser window containing the certificate, copy the URL from the Location or Netsite field.
4. Open a new email message composition window and address it to the requester.
5. Paste the URL into the body of the message, along with instructions to the effect that the user should go to that URL and click the Import button at the bottom of the page.

Alternatively, you can include the URL for the Agent Services gateway in the email message instead, along with the certificate serial number, and instruct the user as follows:

1. Click the Retrieval tab. The List Certificates form should appear.
2. Enter the serial number of the certificate in both serial number fields.
3. Click Find.
4. When the Search Results form appears, click Details.
5. When the certificate appears, scroll down to the bottom of the form and click Import Certificate.

Other Options for Handling Requests

If you do not want to issue the certificate in response to a certificate request, you can choose one of the other options from the command menu at the bottom of the Request Details form, then click Do It.

- **Cancel this request** changes the state of the request to Canceled. Users do not receive automatic notification of cancelled requests. Cancellation can be useful, for example, if the user has left the company since submitting the request, or if you have already talked to the user over the phone about the problem and therefore don’t need to invoke automatic notification.
- **Reject this request** changes the state of the request to Rejected, indicating that it was unacceptable for policy reasons. If the CMS administrator has configured the system to provide automatic notifications to end users, a rejected request will automatically result in such a notification being sent.
- **Clone this request** creates a copy of the request and gives the copy a new request ID number. The status of the new request is Pending. The status of the original request also remains as Pending until you accept, cancel, or reject it.

Chapter 3

Finding and Revoking Certificates

As a Certificate Manager agent, you can use the Agent Services page to find a specific certificate issued by iPlanet Certificate Management Server or to retrieve a list of certificates that match specified criteria. You can examine certificates that you have retrieved. You can also revoke certificates and manage the certificate revocation list.

This chapter has the following sections:

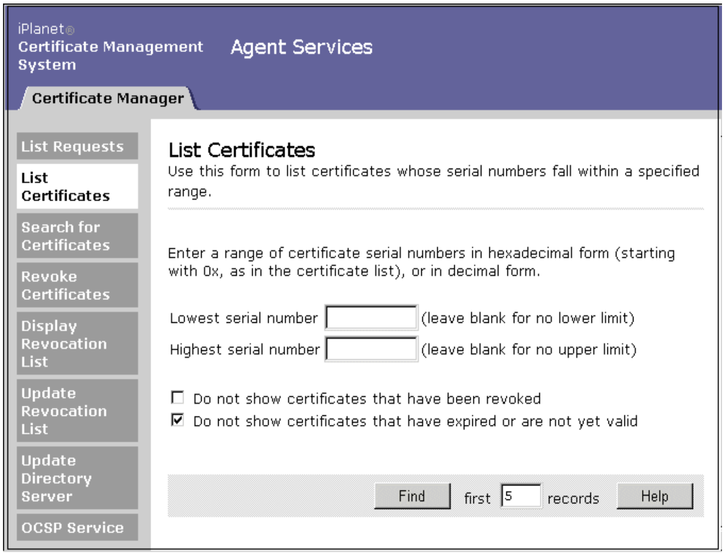
- Basic Certificate Listing (page 45)
- Advanced Certificate Search (page 47)
- Revoking Certificates (page 53)
- Managing the Certificate Revocation List (page 57)

Basic Certificate Listing

You can get a list of certificates quickly and easily by specifying a range of serial numbers. You can also choose to show all certificates within the range, or only those that are currently valid.

To find a specific certificate or to list certificates by serial number:

1. Go to the Certificate Manager Agent Services page (see "Accessing Agent Services" on page 23). You must submit the proper client certificate to get access to this page.
2. Click List Certificates to display the List Certificates form in which you specify listing criteria.



List Certificates

Use this form to list certificates whose serial numbers fall within a specified range.

Enter a range of certificate serial numbers in hexadecimal form (starting with 0x, as in the certificate list), or in decimal form.

Lowest serial number (leave blank for no lower limit)

Highest serial number (leave blank for no upper limit)

☐ Do not show certificates that have been revoked

☑ Do not show certificates that have expired or are not yet valid

3. To find a certificate with a specific serial number, enter the serial number in both the upper limit and lower limit fields of the List Certificates form, in either decimal or hexadecimal form.

   Use `0x` to indicate the beginning of a hexadecimal number; for example, `0x00000006`. (Serial numbers are displayed in hexadecimal form in the Search Results and Details pages.)

4. To find all certificates within a range of serial numbers, enter the upper and lower limits of the serial number range (in decimal or hexadecimal form).

   If you leave either the lower limit or upper limit field blank, the certificate whose number you specified plus all certificates before or after it in sequence are displayed.

5. To limit the returned list to valid certificates, select one or both of the checkboxes labeled with filtering methods.

   You can choose not to show revoked certificates or not to show certificates that have expired or are not yet valid.

6. Enter the number of certificates matching the criteria that you want to see.

   For a number *n*, the first *n* matching certificates are initially displayed.

7. Click Find.

   Certificate Management System displays a list of the certificates that match your search criteria. You can select a certificate in the list and examine it in more detail or perform various operations on it. For more information, see “Examining Certificates” on page 52.

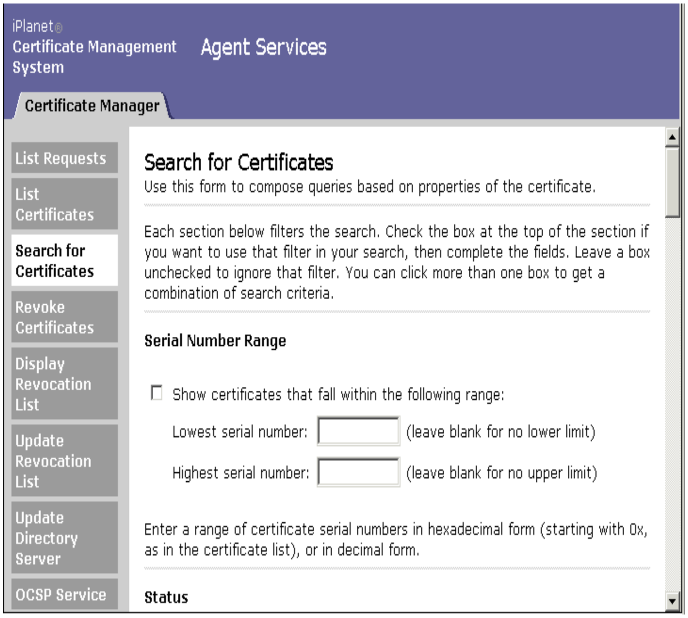
Advanced Certificate Search

If you want to search for certificates by more complex criteria than serial number, use the advanced search form.

To perform an advanced search for certificates:

1. Go to the Certificate Manager Agent Services page (see “Accessing Agent Services” on page 23). You must submit the proper client certificate to get access to this page.

2. Click Search for Certificates to display the Search for Certificates form in which you specify search criteria.



Search for Certificates

Use this form to compose queries based on properties of the certificate.

Each section below filters the search. Check the box at the top of the section if you want to use that filter in your search, then complete the fields. Leave a box unchecked to ignore that filter. You can click more than one box to get a combination of search criteria.

Serial Number Range

□ Show certificates that fall within the following range:

Lowest serial number: (leave blank for no lower limit)

Highest serial number: (leave blank for no upper limit)

Enter a range of certificate serial numbers in hexadecimal form (starting with 0x, as in the certificate list), or in decimal form.

Status

3. To search by particular criteria, use one or more of the sections of the Search for Certificates form.

   The form is quite long; scroll down to see the different sections. To use a section, select the appropriate checkbox, then fill in any necessary information.

   Serial Number Range. Use this section to find a certificate with a specific serial number or to list all certificates within a range of serial numbers.

   - To find a certificate with a specific serial number, enter the serial number in both the upper limit and lower limit fields, in either decimal or hexadecimal form. Use `0x` to indicate the beginning of a hexadecimal number; for example, `0x2A`. (Serial numbers are displayed in hexadecimal form in the Search Results and Details pages.)
   - To find all certificates within a range of serial numbers, enter the upper and lower limits of the serial number range (in decimal or hexadecimal form).

     If you leave either the lower limit or upper limit field blank, all certificates before or after the one you specify are displayed.

   Status. Use this section to select certificates by their status. A certificate can have one of the following status codes:

   - VALID **-** The certificate has been issued, its validity period has begun but not ended, and it has not been revoked.
   - INVALID **-** The certificate has been issued, but its validity period has not yet begun.
   - REVOKED **-** The certificate has been revoked.
   - EXPIRED **-** The current time is later than the end of the certificate's validity period.
   - REVOKED & EXPIRED **-** The certificate meets the criteria for both status codes.

   Subject Name. Use this section to list certificates with a particular owner. For more information on filling in this section, see Step 4.

   Revocation Information. Use this section to list certificates that have been revoked during a particular period or by a particular agent. For example, you can list all certificates revoked between July 1996 and January 1997, or all certificates revoked by the agent with the user name `admin`.

- To list certificates revoked within a time period, select the day, month, and year from the drop-down lists to identify the beginning and end of the period.
- To list certificates revoked by a particular agent, enter the name of the agent. You can use wildcards in this field. (For more information on wildcard syntax, see Step 4.)

Issuing Information. Use this section to list certificates that have been issued during a particular period or by a particular agent. For example, you can list all certificates issued between July 1996 and January 1997, or all certificates issued by the agent with the user name `betatest`.

- To list certificates issued within a time period, select the day, month, and year from the drop-down lists to identify the beginning and end of the period.
- To list certificates issued by a particular agent, enter the name of the agent. You can use wildcards in this field. (For more information on wildcard syntax, see Step 4.)

Dates of Validity. Use this section to list certificates that become effective or expire during a particular period. For example, you can list all certificates that became valid on June 1, 1996, or that expired between January 1, 1997 and June 1, 1997.

You can also list certificates that have a validity period of a certain length of time. For example, you can list all certificates that are valid for less than one month.

- To list certificates that become effective or expire within a time period, select the day, month, and year from the drop-down lists to identify the beginning and end of the period.
- To list certificates that have a validity period of a certain length in time, select "not greater than" or "not less than" from the drop-down list, enter a number, and select a time unit from the drop-down list: Days, Weeks, Months, or Years.

Type. Use this section to list certain types of certificates. For example, you can list all certificates for subordinate CAs. Note that this search works only for certificates containing the `netscape-cert-type` extension, which stores type information.

- For each type, choose from the drop-down list to find certificates where that type is On, Off, or Absent.

4. To find a certificate with a specific subject name, use the Subject Name section.

   - Select the checkbox, then enter the subject name criteria.
   - Enter values for the fields you want included in your search criteria and leave the others blank.

   The standard tags or components are as follows:

   Email address. To narrow the search by email address, enter the email address in this field.

   Common name. To find certificates associated with a specific person or server, enter the name in this field.

   UserID. The user id for the person whose certificate you want to find. For example, at many companies the user id is the name used to log in to the network when starting up a computer.

   Organization unit. To narrow the search to a specific division, department, or unit within an organization, enter the name of the unit in this field.

   Organization. To narrow the search by organization, enter the name of the business, university, or organization in this field.

   Locality. To narrow the search by locality, enter the name of the local area (for example, the name of the city) in this field.

   State. To narrow the search by state or province, enter the name of the state or province in this field.

   Country. To narrow the search by country, enter the two-letter code for the country (for example, `US`) in this field.

   When you have entered the field values for the server to match, specify the type of search that you want performed:

   - Select Exact to search for certificates that have subject names that match exactly the components you have specified and contain none of the components you have left blank. You cannot use wildcards in this type of search.

- Select Partial to search for all certificates with subject names that match at least the components you have specified but that may also have any values in the components you have left blank.

  You can specify wildcard patterns in this type of search by using the question mark character (?) to match an arbitrary single character and the asterisk character (*) to match an arbitrary string of zero or more characters.

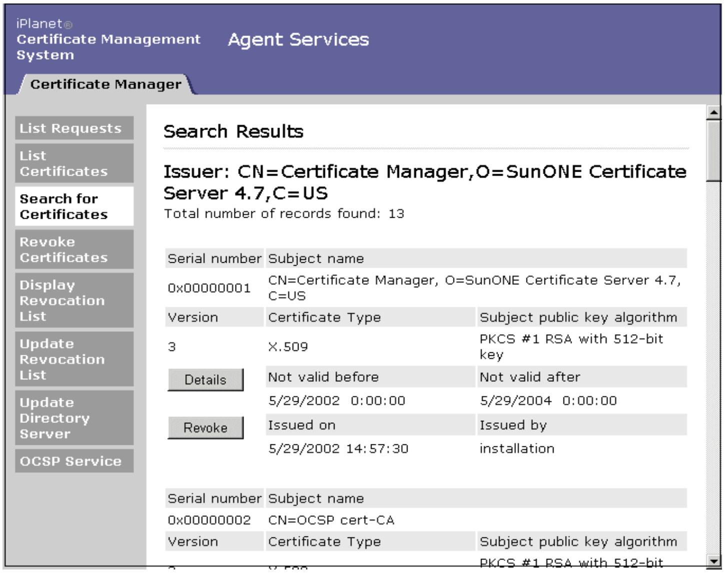
  Note that placing a single asterisk in a given field in the search form specifies that the corresponding component must be in the certificate's subject name but may have any value whatsoever. To indicate that you do not care if the component is present, leave the field blank.

5. After entering your search criteria, scroll to the bottom of the form and enter the number of certificates matching your specified criteria that you want to see.

   For a number *n*, the first *n* matching certificates are initially displayed.

6. Click Find.

   The Search Results form appears, showing a list of the certificates that match your search criteria. You can select a certificate in the list and examine it in more detail. For more information, see "Examining Certificates" on page 52.



Search Results

Issuer: CN=Certificate Manager,O=SunONE Certificate Server 4.7,C=US
Total number of records found: 13

Serial number	Subject name	
0x00000001	CN=Certificate Manager, O=SunONE Certificate Server 4.7, C=US	
Version	Certificate Type	Subject public key algorithm
3	X.509	PKCS #1 RSA with 512-bit key
Details	Not valid before	Not valid after
	5/29/2002 0:00:00	5/29/2004 0:00:00
Revoke	Issued on	Issued by
	5/29/2002 14:57:30	installation
Serial number	Subject name	
0x00000002	CN=OCSP cert-CA	
Version	Certificate Type	Subject public key algorithm
		PKCS #1 RSA with 512-bit

Examining Certificates

To examine the details of a certificate, follow these steps:

1. On the Agent Services page, click List Certificates or Search for Certificates, specify search criteria, and click Find to display a list of certificates.

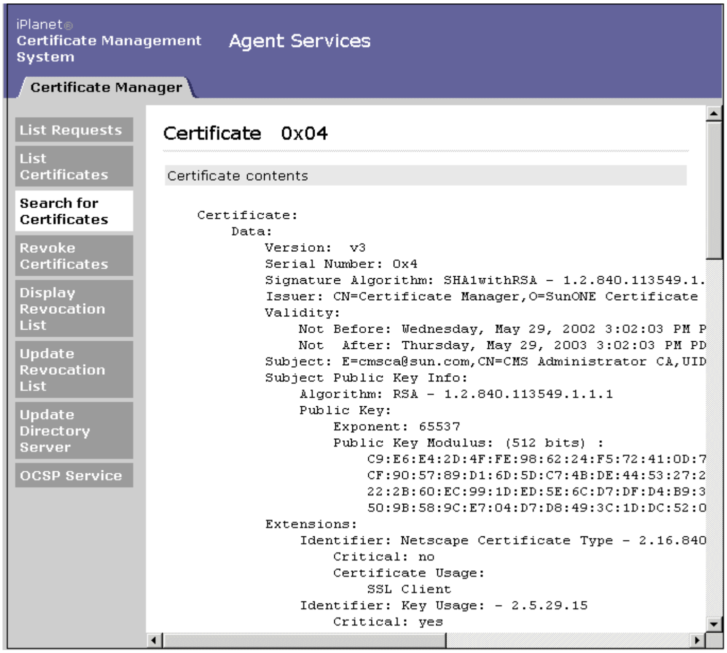
   For details of how to specify criteria, see "Basic Certificate Listing" on page 45 and "Advanced Certificate Search" on page 47.

2. On the Search Results form, find the particular certificate you want to examine.

   If the certificate you want to see is not shown, scroll to the bottom of the list, specify an additional number *n*, and click Find. The system displays the next *n* certificates that match your original search criteria.

3. When you have found the certificate you want, click the Details button at the left side of its entry.

   The Certificate page appears. It shows the detailed contents of the selected certificate and instructions for installing the certificate in a server or in Netscape Communicator.



Certificate 0x04

Certificate contents

```
Certificate:
    Data:
        Version:  v3
        Serial Number: 0x4
        Signature Algorithm: SHA1withRSA - 1.2.840.113549.1.
        Issuer: CN=Certificate Manager,O=SunONE Certificate
        Validity:
            Not Before: Wednesday, May 29, 2002 3:02:03 PM P
            Not  After: Thursday, May 29, 2003 3:02:03 PM PD
        Subject: E=cmsca@sun.com,CN=CMS Administrator CA,UID
        Subject Public Key Info:
            Algorithm: RSA - 1.2.840.113549.1.1.1
            Public Key:
                Exponent: 65537
                Public Key Modulus: (512 bits) :
                    C9:E6:E4:2D:4F:FE:98:62:24:F5:72:41:0D:7
                    CF:90:57:89:D1:6D:5D:C7:4B:DE:44:53:27:2
                    22:2B:60:EC:99:1D:ED:5E:6C:D7:DF:D4:B9:3
                    50:9B:58:9C:E7:04:D7:D8:49:3C:1D:DC:52:0
        Extensions:
            Identifier: Netscape Certificate Type - 2.16.840
                Critical: no
                Certificate Usage:
                    SSL Client
            Identifier: Key Usage: - 2.5.29.15
                Critical: yes
```

The certificate is shown in base-64 encoded form at the bottom of the Certificate page, under the heading “Installing this certificate in a server.” In addition to its use with servers, this encoded form of the certificate can be used by CMS administrators and Data Recovery Manager agents for setting up new agents and recovering private encryption keys, respectively. (For more information on key recovery, see “Finding and Recovering Keys” on page 65 in Chapter 5.)

Revoking Certificates

Only Certificate Manager agents can revoke certificates other than their own. You need to revoke a certificate if one of the following situations occurs:

- The owner of the certificate has changed status and no longer has the right to use the certificate.
- The private key of a certificate owner has been compromised.

To revoke one or more certificates, you must search for the certificates you want to revoke using the Revoke Certificates button. While the search is similar to the one invoked by Search for Certificates, the Search Results form returned by this search gives you the option of revoking one or all of the found certificates.

Searching for Certificates to Revoke

To search for one or more certificates to revoke:

1. Go to the Certificate Manager Agent Services page (see “Accessing Agent Services” on page 23).

   You must submit the proper client certificate to get access to this page.

2. Click Revoke Certificates.

   The search form that appears has the same search criteria sections as the Search for Certificates form.

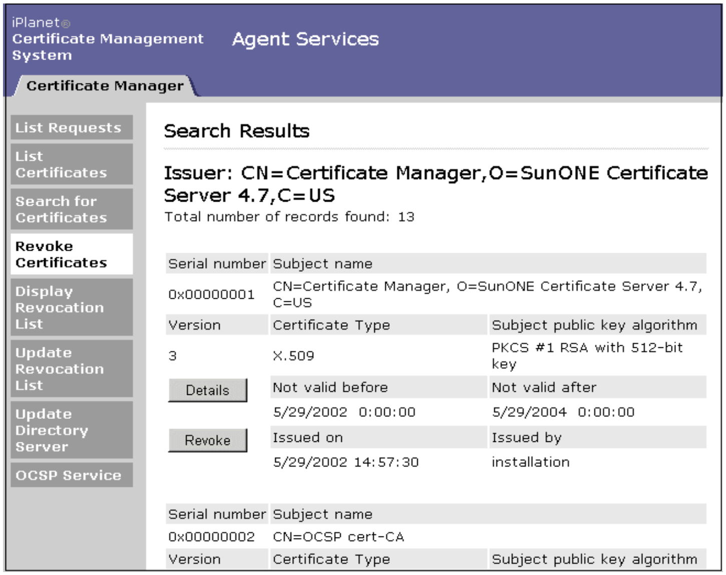
3. Specify the search criteria by selecting the checkboxes for the sections you want to use, then filling in the required information.

   For details on search criteria, see “Advanced Certificate Search” on page 47.

4. Scroll to the bottom of the form and select a number of matching certificates to display.

5. Click Find.

   The search returns a list of matching certificates. You have the option of revoking one or all certificates in the list.



Search Results

Issuer: CN=Certificate Manager,O=SunONE Certificate Server 4.7,C=US

Total number of records found: 13

Serial number	Subject name	
0x00000001	CN=Certificate Manager, O=SunONE Certificate Server 4.7, C=US	
Version	Certificate Type	Subject public key algorithm
3	X.509	PKCS #1 RSA with 512-bit key
Details	Not valid before	Not valid after
	5/29/2002 0:00:00	5/29/2004 0:00:00
Revoke	Issued on	Issued by
	5/29/2002 14:57:30	installation
Serial number	Subject name	
0x00000002	CN=OCSP cert-CA	
Version	Certificate Type	Subject public key algorithm

Revoking One or More Certificates

You can revoke an entire list of certificates returned by a search, or select and revoke one of the certificates from the list.

Revoking One Certificate

To revoke a single certificate:

1. On the Certificate Manager’s Agent Services page, click Revoke Certificates, specify search criteria, and click Find to display a list of certificates.

   For details of how to specify criteria, see “Basic Certificate Listing” on page 45 and “Advanced Certificate Search” on page 47.

2. On the Search Results form, find the certificate you want to revoke.

   If the certificate you want to see is not shown, scroll to the bottom of the list, specify an additional number *n*, and click Find. The system displays the next *n* certificates that match your original search criteria.

3. Click the Revoke button next to the certificate that you want to revoke.

4. Confirm the revocation in the resulting form (see “Confirming a Revocation” on page 55).

Revoking Multiple Certificates

To revoke all of the certificates found by a search:

1. On the Certificate Manager’s Agent Services page, click Revoke Certificates, specify search criteria, and click Find to display a list of certificates.

   For details of how to specify criteria, see “Basic Certificate Listing” on page 45 and “Advanced Certificate Search” on page 47.

2. On the Search Results page, scroll to the bottom to reach the "Revoke ALL *n* Certificates" button. The number shown in the button is the total number of certificates returned by the search. Note that this is usually a larger number than the number of certificates displayed on the current page.

3. Verify that all of the certificates returned by the search should be revoked (not just those displayed on the current page).

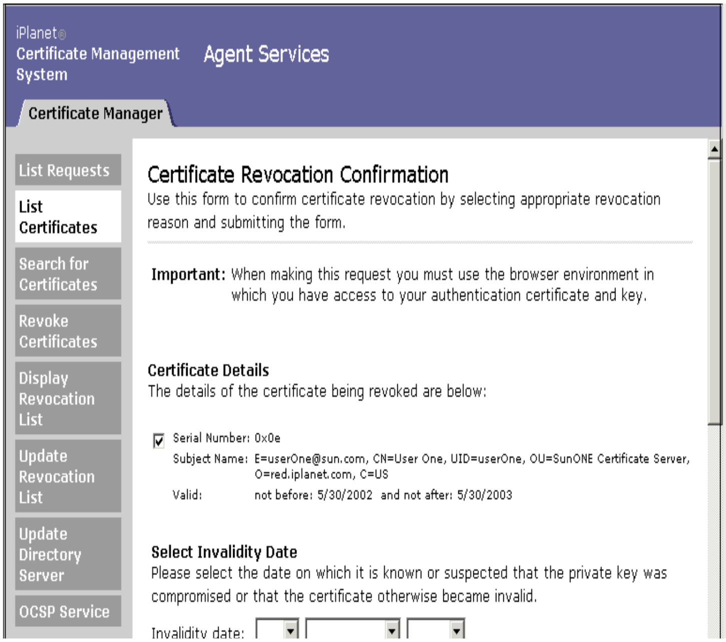
4. Click "Revoke ALL *n* Certificates" at the bottom of the form.

5. Confirm the revocation in the resulting form (see “Confirming a Revocation” on page 55).

CAUTION Whether you are revoking a single certificate or a list of certificates, be extremely careful that you have selected the correct one or that the list contains only the certificates you want to revoke. Once you confirm a revocation operation, there is no way to undo it.

Confirming a Revocation

When you have requested the revocation of one or more certificates, the Certificate Revocation Confirmation form appears.



Certificate Revocation Confirmation

Use this form to confirm certificate revocation by selecting appropriate revocation reason and submitting the form.

Important: When making this request you must use the browser environment in which you have access to your authentication certificate and key.

Certificate Details

The details of the certificate being revoked are below:

☑ Serial Number: 0x0e
Subject Name: E=userOne@sun.com, CN=User One, UID=userOne, OU=SunONE Certificate Server, O=red.iplanet.com, C=US
Valid: not before: 5/30/2002 and not after: 5/30/2003

Select Invalidity Date

Please select the date on which it is known or suspected that the private key was compromised or that the certificate otherwise became invalid.

Invalidity date:

To confirm the revocation:

1. Inspect the details of the certificate and verify that it is the one you want to revoke. If you are revoking more than one certificate, the form shows details of all the listed certificates.
2. Select a reason for the revocation. The reason applies to all the listed certificates.
3. Optionally, enter any additional comment. The comment will be included in the revocation request.
4. Click Submit.

   The revocation request is submitted; it is automatically approved, and the certificate is revoked. You can see revocation requests by listing requests with a status of Completed.

CAUTION Whether you are revoking a single certificate or a list of certificates, be extremely careful that you have selected the correct one or that the list contains only the certificates you want to revoke. Once you confirm a revocation operation, there is no way to undo it.

Managing the Certificate Revocation List

By revoking a certificate, you are notifying other users that the certificate is no longer valid. You make this notification by publishing a list of the revoked certificates, called the *certificate revocation list* (CRL), to an LDAP directory. This list is publicly available and ensures that revoked certificates are not misused.

NOTE	Certificate Management System is currently the only iPlanet server that can check the revocation status of the certificates that it issues. With Certificate Management System, therefore, you can use the certificate revocation status to control access. On other iPlanet servers, you must use other forms of access control. For example, you can remove individual users from access groups to prevent them from accessing the server.

Viewing or Examining CRLs

In some cases, you may need to view or examine the CRL, for example, prior to manually updating the directory with the latest CRL.

Only a Certificate Manager agent can view the CRL.

To view or display the CRL:

1. Go to the Certificate Manager Agent Services page (see “Accessing Agent Services” on page 23). You must submit the proper client certificate to get access to this page.
2. Click Display Certificate Revocation List to display the form for viewing the CRL.
3. Select the CRL that you want to view. (If your administrator has created multiple issuing points, you will see them in the “Issuing point” drop-down list. Otherwise, you’ll only see the master CRL.)
4. To examine the selected CRL, click Display.

   The CRL appears in the browser window. You can, for example, check whether a particular certificate appears in the list. Additionally, you can also can note recent changes: total number of certificates that were revoked since the last update, total number of certificates that were taken off hold since the last update, and total number of certificates that expired since the last update.

Updating the CRL

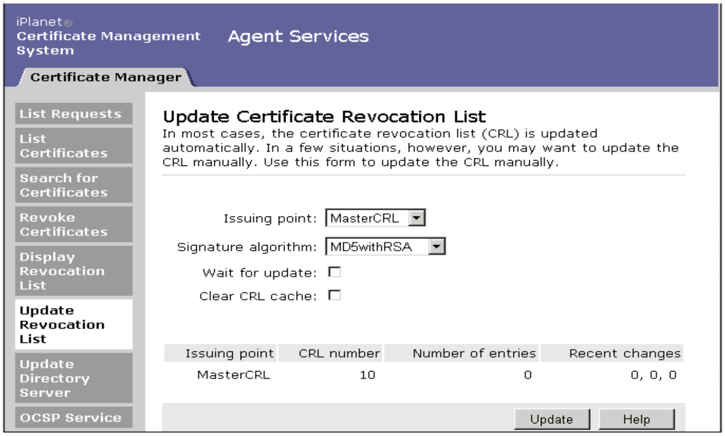
Normally, when you revoke a certificate, the CRL is automatically updated. If you are using Certificate Management System with an LDAP directory server, the CRL in the directory is updated automatically.

In some cases, you need to update the CRL manually. For example, you might want to remove expired certificates from the CRL to reduce its size. (Expired certificates do not need to be included in the CRL; they are already invalid because of the expiration date.) You might also want to update the CRL manually after the system has been down for any reason.

Only a Certificate Manager agent can manually update the CRL.

To manually update the CRL:

1. Go to the Certificate Manager Agent Services page (see “Accessing Agent Services” on page 23). You must submit the proper client certificate to get access to this page.
2. Click Update Revocation List to display the form for updating the CRL.



Update Certificate Revocation List

In most cases, the certificate revocation list (CRL) is updated automatically. In a few situations, however, you may want to update the CRL manually. Use this form to update the CRL manually.

Issuing point: MasterCRL

Signature algorithm: MD5withRSA

Wait for update: □

Clear CRL cache: □

Issuing point	CRL number	Number of entries	Recent changes
MasterCRL	10	0	0, 0, 0

3. Select the algorithm that you want to use to sign the new CRL.

   - MD5 with RSA generates a 128-bit message digest. Most existing software applications that handle certificates support only MD5. This is the default algorithm.
   - SHA-1 with RSA generates a 160-bit message digest. Before choosing SHA-1 with RSA, make sure your applications support it. Netscape Navigator 3.0 (or later) and Enterprise Server 2.01 (or later) support SHA-1.

- SHA-1 with DSA generates a 160-bit message digest. Before choosing SHA-1 with DSA, make sure your applications support it. Communicator 4.0 (or later) and iPlanet server products with a version number greater than 4.0 support it.

Before selecting an algorithm, make sure that Certificate Management System has the algorithm enabled. Your CMS administrator can let you know whether this is the case.

4. To examine CRL before updating it, click Display.

   The CRL appears in the browser window. You can, for example, check whether a particular certificate appears in the list. Use the browser's Back button to return to the Update page.

5. To update the CRL with the latest certificate revocation information, click Update.

Chapter 4

Publishing to a Directory

This chapter describes the procedures for updating an LDAP directory with the current status of certificates. Only a Certificate Manager agent can update the directory.

The chapter has the following sections:

- Working with a Directory Server (page 61)
- Updating the Directory with Changes (page 62)

Working with a Directory Server

If your organization uses iPlanet Directory Server (or another LDAP directory server) to publish information about users in your organization, you can configure Certificate Management System to publish certificates and certificate revocation lists through the directory.

Certificate information published to the directory must be periodically updated as certificates are issued and revoked. Updates are usually published automatically but can also be published manually.

Automatic Directory Updates

Once the CMS administrator has configured Certificate Management System to work with Directory Server, any changes to certificate information in Certificate Management System are automatically updated in the directory. Updates take place at specific times:

- The first time you start Certificate Management System, it publishes the Certificate Manager’s CA certificate to the directory.

- When Certificate Management System issues a new certificate, the certificate is published to the directory.
- When Certificate Management System revokes a certificate, the certificate is removed from the directory.
- When the CRL is created or updated, the list is published to the directory.

Manual Directory Updates

Normally you do not need to update a directory manually; most updates are done automatically. You must update the directory manually in the following situations:

- Directory Server is down for a period of time and unable to receive changes from Certificate Management System.
- You want to remove expired certificates from the directory. Expired certificates are not automatically removed from the directory upon expiration. (Generally, any client using a certificate is responsible for determining that it is valid by checking its expiration date against the client's current date information.)

Using the Update Directory Server form available from the Certificate Manager Agent Services page, you make the following changes in the directory:

- Update the CRL in the directory.
- Update information on valid certificates (for example, update the server with newly issued certificates or recently renewed certificates).
- Remove expired certificates.
- Remove revoked certificates.

Note that only a Certificate Manager agent with the proper certificate can access the Update Directory Server form.

Updating the Directory with Changes

To manually update the directory with changes:

1. Go to the Certificate Manager Agent Services page (see "Accessing Agent Services" on page 23). You must submit the proper client certificate to get access to this page.
2. Click Update Directory Server.

3. Select “Skip certificates already marked as updated” to ignore certificates in the internal database that are maked as having been published already (or removed in the case of revoked certificates).

   For example, if you updated the directory once to revoke many certificates and it took several minutes, some new certificates may have been issued while the update was running. You would then use this selection and update the directory a second time to publish the new certificates (and save time by skipping all of the certificates that were just updated).

4. To publish the latest CRL, select "Update certificate revocation list to the directory."

5. To update information on valid certificates to the directory, select “Update valid certificates to the directory.”

   If you want to update only a range of certificates (for example, only the most recently issued certificates), specify the range of the serial numbers of those certificates.

6. To remove expired certificates from the directory, select “Remove expired certificates from the directory.”

   If you want to remove only a range of certificates (not all expired certificates), specify the range of the serial numbers of those certificates.

7. To remove revoked certificates from the directory, select “Remove revoked certificates from the directory.”

   If you want to remove only a range of certificates (not all revoked certificates), specify the range of the serial numbers of those certificates.

8. When you have finished specifying the changes that you want updated, click Update Directory.

NOTE In some circumstances, updating the directory can take considerable time. During this period, any changes made through Certificate Management System (for example, any new certificates issued or any certificates revoked) may not be included in the update. If you have issued or revoked any certificates during that time, you need to update the directory again to reflect those changes. Use “Skip certificates already marked as updated” the second time to update only certificates that changed (issued, revoked, expired) while the previous update was running.

Chapter 5

Recovering Encrypted Data

This chapter describes how to process key recovery requests and how to recover stored encrypted data when the encryption key has been lost. This service is available only when the Data Recovery Manager subsystem is installed. The Data Recovery Manager Agent Services page allows certified agents to accomplish these tasks.

This chapter has the following sections:

Finding and Recovering Keys

If an end user loses a private encryption key or if a key's owner is unavailable, data encrypted with that key cannot be read unless a copy of the private key was archived when the key was created. The archived key can then be recovered and used to read the data.

As a Data Recovery Manager agent, you manage key recovery using the Data Recovery Manager's Agent Services page. You can search through archived keys, either to view them or to initiate a key recovery. Once you have initiated key recovery, a minimum number of designated key recovery agents are required to authorize the recovery. Key recovery agents may or may not also be certified Data Recovery Manager agents.

Finding Archived Keys

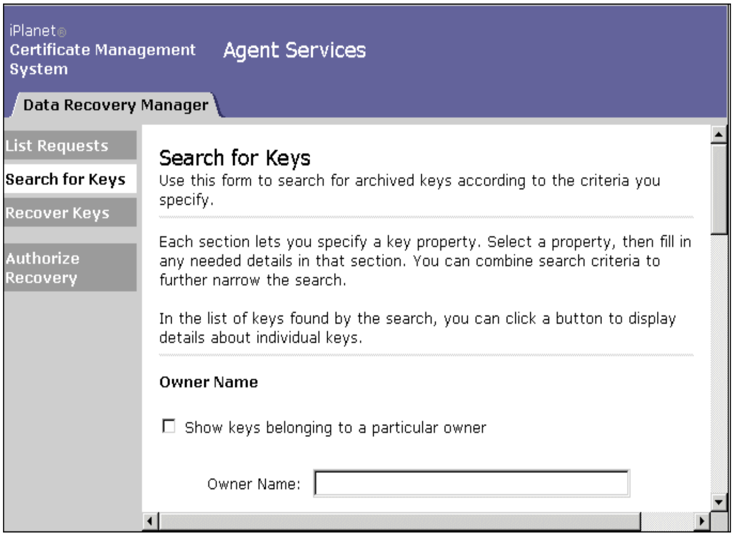
You can search for archived keys to examine them or to initiate recovery. The process of selecting search criteria and selecting a key from the search results is the same in either case.

To search for and list archived keys:

1. Go to the Data Recovery Manager Agent Services page (see "Accessing Agent Services" on page 23).You must submit the proper client certificate to get access to this page.

2. Click Search for Keys or Recover Keys to display the form in which you specify search criteria.

   If you choose Recover Keys, you will have the option of initiating recovery for any key that you find.



Search for Keys

Use this form to search for archived keys according to the criteria you specify.

Each section lets you specify a key property. Select a property, then fill in any needed details in that section. You can combine search criteria to further narrow the search.

In the list of keys found by the search, you can click a button to display details about individual keys.

Owner Name

□ Show keys belonging to a particular owner

Owner Name:

3. To search by particular criteria, use one or more of the different sections of the Search for Keys or Recover Keys form. To use a section, select the appropriate checkbox in that section, then fill in any necessary information.

   Owner Name. Use this section to find an archived key with a specific owner name. The owner name for a key is much like the subject name for a certificate. It consists of a string that can be used in searches. Select the checkbox and enter the owner name for the key you want to find.

Key identifiers. Use this section to find an archived key with a specific key identifier or to list all keys within a range of key identifiers.

- To find a key with a specific key identifier, enter the key identifier in both the upper limit and lower limit fields. Use decimal or hexadecimal form. Use `0x` to indicate the beginning of a hexadecimal number; for example, `0x2A`. (Key identifiers are displayed in hexadecimal form in the Search Results and Details pages.)
- To find all keys within a range of key identifiers, enter the upper and lower limits of the key identifier range (in decimal or hexadecimal form).

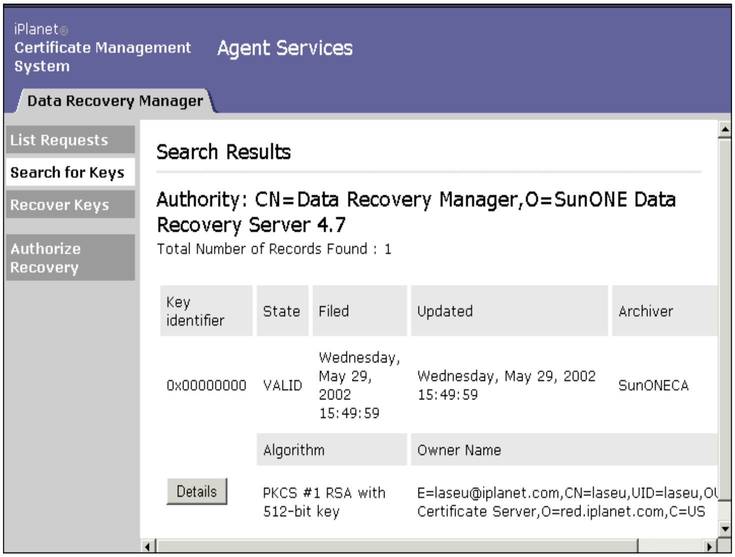
  If you leave either the lower limit or upper limit field blank, all keys before or after the one you specify are displayed.

Certificate. Use this section to find the archived key that corresponds to a specific public key. Select the checkbox and paste the certificate containing the corresponding public key (in base-64 encoded form) into the text area. (You must first find and copy the encoded form of the encryption certificate associated with the key pair. Use the Certificate Manager or Registration Manager Agent Services pages to find the certificate; for instructions, see “Examining Certificates” on page 52 in Chapter 3.)

Archiver. Use this section to find keys that were archived by a specific server. Select the checkbox and enter the user ID of the Certificate Manager or Registration Manager that submitted the key archival request. Note that this information is available only for archival requests from servers that are remote from the Data Recovery Manager (that is, not installed in the same server root directory).

4. After entering your search criteria, click Show Key.

   The Data Recovery Manager displays a list of the keys that match your search criteria. You can select a key in the list and examine it in more detail (described in “Selecting a Key” on page 68). If you initiated the search with the Recover Keys button, you have the option of recovering any key returned by the search (described in “Recovering Keys” on page 69).



Search Results

Authority: CN=Data Recovery Manager,O=SunONE Data Recovery Server 4.7

Total Number of Records Found : 1

Key identifier	State	Filed	Updated	Archiver
0x00000000	VALID	Wednesday, May 29, 2002 15:49:59	Wednesday, May 29, 2002 15:49:59	SunONECA
	Algorithm		Owner Name	
Details	PKCS #1 RSA with 512-bit key		E=laseu@iplanet.com,CN=laseu,UID=laseu,O Certificate Server,O=red.iplanet.com,C=US	

Selecting a Key

To select a key from the list returned by your key search:

1. On the Data Recovery Manager's Agent Services page, click Search for Keys, specify search criteria, and click Show Key to display a list of archived keys.

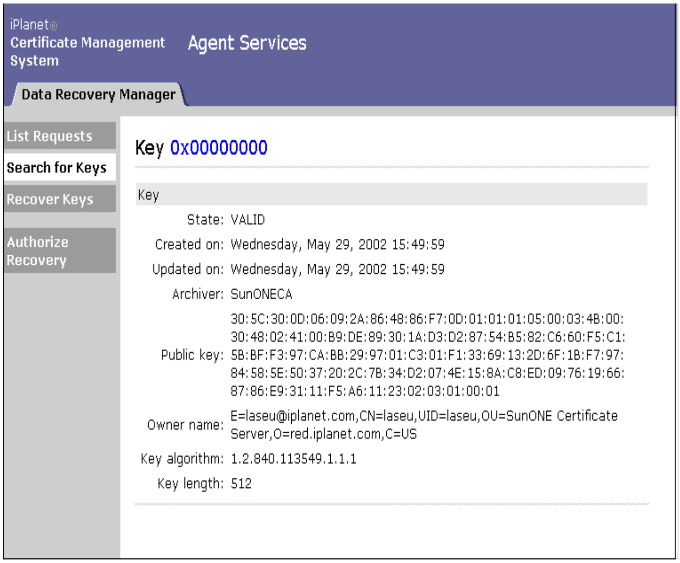
   For details, see "Finding Archived Keys" on page 66.

2. On the Search Results form, find a particular key.

   If the key you want to see is not shown, scroll to the bottom of the list and select the Next or Previous group of keys.

3. Click Details next to the key you want to examine.

   The details of the selected key are shown in the Key details page. You cannot manipulate the key in any way.



Key 0x00000000

Key	
State:	VALID
Created on:	Wednesday, May 29, 2002 15:49:59
Updated on:	Wednesday, May 29, 2002 15:49:59
Archiver:	SunONECA
Public key:	30:5C:30:0D:06:09:2A:86:48:86:F7:0D:01:01:01:05:00:03:4B:00: 30:48:02:41:00:B9:DE:89:30:1A:D3:D2:87:54:B5:82:C6:60:F5:C1: 5B:BF:F3:97:CA:BB:29:97:01:C3:01:F1:33:69:13:2D:6F:1B:F7:97: 84:58:5E:50:37:20:2C:7B:34:D2:07:4E:15:8A:C8:ED:09:76:19:66: 87:86:E9:31:11:F5:A6:11:23:02:03:01:00:01
Owner name:	E=laseu@iplanet.com,CN=laseu,UID=laseu,OU=SunONE Certificate Server,O=red.iplanet.com,C=US
Key algorithm:	1.2.840.113549.1.1.1
Key length:	512

Recovering Keys

If you perform a search with the Recover Keys button, the Search Results form allows you to initiate the recovery of any key found.

To initiate key recovery:

1. On the Data Recovery Manager's Agent Services page, click Recover Keys, specify search criteria, and click Show Key to display a list of archived keys.

   For details, see "Finding Archived Keys" on page 66.

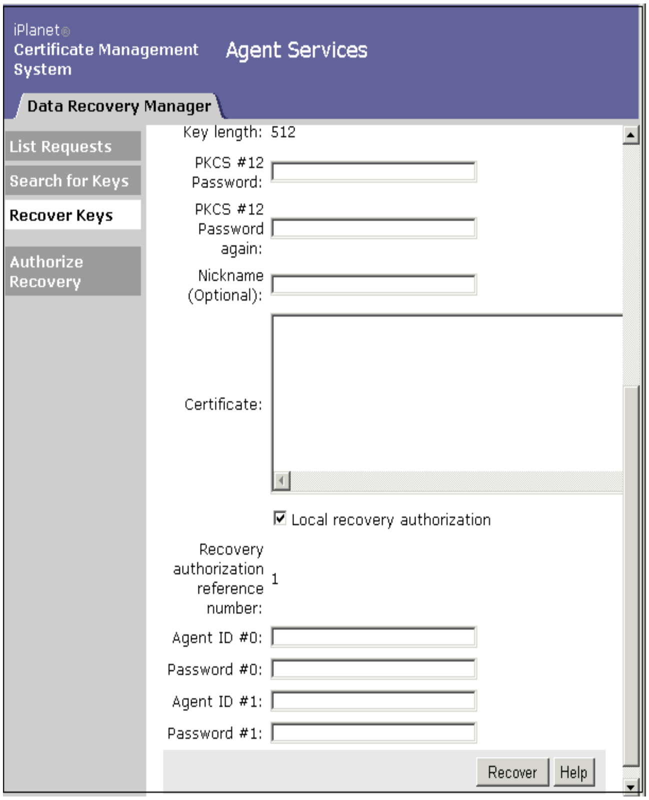
2. On the Search Results form, find a particular key.

   If the key you want to see is not shown, scroll to the bottom of the list and select the Next or Previous group of keys.

3. Click Recover next to the key you want to examine.

   The details of the selected key are displayed in the Authorize Key Recovery form, which allows you to specify authorization information.

4. In the Key Recovery form, scroll to the bottom of the key information.



Key length: 512

PKCS #12 Password:

PKCS #12 Password again:

Nickname (Optional):

Certificate:

☑ Local recovery authorization

Recovery authorization reference number: 1

Agent ID #0:

Password #0:

Agent ID #1:

Password #1:

The number of key recovery agent authorizations required to recover a key is configured by the system administrator using the CMS window in iPlanet Console. The Key Recovery form has space for the required number of authorizations.

5. Specify the password that the requester will use in importing the recovered certificate / key pair package.

6. Paste the base-64 encoded certificate that corresponds to the archived key into the text area.

   Use the Certificate Manager or Registration Manager Agent Services pages to find and copy the certificate; see “Examining Certificates” on page 52 in Chapter 3.

   If you searched for the archived key by using the corresponding public key, the certificate information is automatically transferred here.

7. Choose whether to authorize recovery locally.
   - If you select this option, assemble the required number of key recovery agents and have each agent fill in his or her user name and password.
   - If you deselect this option, notify the key recovery agents that a recovery has been initiated, giving them the recovery authorization reference number indicated on this form. (For information on how to provide a remote authorization, see “Remote Recovery Authorization” on page 71.)
8. Click Recover Now.
   - If you chose local authorization, the recovery is completed immediately, and the recovered certificate and key pair are sent to your browser in the form of a PKCS #12 package.
   - If you chose remote authorization, you must wait for the recovery agents to enter their authorizations. As they do so, a status page informs you of the progress. When the required number of recovery agents have completed their authorizations, the recovery is completed and the recovered certificate / key pair package is sent to your browser.
9. In the dialog box that appears, specify the path and filename for saving the encrypted file that contains the recovered certificate and key pair.
10. Send the encrypted file to the requesting party.
11. Inform the requesting party of the recovery password in a secure manner.

    The recovering party must use this password to import the recovered certificate / key pair package into his or her client software.

Remote Recovery Authorization

By default, recovery authorization is local. That is, when you initiate the recovery, you assemble the required number of recovery agents, and all of them enter their IDs and passwords on the same Authorize Key Recovery form on your system. When you click Recover Now, the recovery is completed, and you receive the encrypted file that contains the recovered key and certificate.

If you deselect the local authorization option, you are choosing remote authorization. When you click Recover Now, the key recovery agents must each access the Data Recovery Manager Agent Services pages at their own locations, and use the Authorize Recovery button to enter each authorization separately. You are informed of the status of the authorizations. When all the authorizations have been entered, the recovery is completed and you receive the encrypted file that contains the recovered key and certificate.

To use the remote authorization feature, the designated key recovery agents must also be designated Data Recovery Manager agents, so that they are privileged to access the Agent Services pages directly. If you are using only local authorization, anyone can be designated as a recovery agent, since only you will need to access the recovery authorization form.

If you are a designated key recovery agent as well as a Data Recovery Manager agent, and another Data Recovery Manager agent informs you that a remote key recovery authorization has been initiated, enter your authorization as follows:

1. Go to the Data Recovery Manager Agent Services page (see “Accessing Agent Services” on page 23). You must submit the proper client certificate to get access to this page.
2. Click Authorize Recovery.
3. Enter the recovery authorization reference number that was part of the notification.

   This number identifies the particular key recovery request that you are to authorize.
4. Click Examine.
5. Enter your key recovery agent ID and password.
6. Click OK.

The initiating agent is informed that you have completed your authorization.

Viewing Key Service Requests

Key service requests are of two kinds:

- Key archival requests, made by remote or local Certificate Managers or Registration Managers
- Key recovery requests, made by Data Recovery Manager agents

As a Data Recovery Manager agent, you can view these requests. You can search for and list key service requests with a particular status, such as completed or rejected. You can select a key service request from the returned list and examine it in detail.

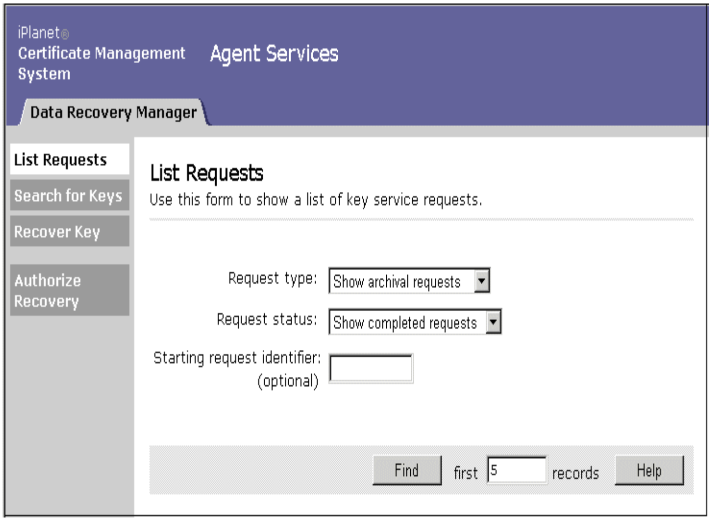
Key service requests are usually handled internally. You do not need to take any action on them unless your system is specially configured.

Listing Key Service Requests

To list key service requests:

1. Go to the Data Recovery Manager Agent Services page (see "Accessing Agent Services" on page 23). You must submit the proper client certificate to get access to this page.

2. Click List Requests to display the List Requests form.



List Requests

Use this form to show a list of key service requests.

Request type: Show archival requests

Request status: Show completed requests

Starting request identifier: (optional)

first 5 records

Use the List Requests form to specify which key service requests to list.

3. Choose the type of requests you want to see from the "Request type" pull-down menu. You can choose to see requests to archive keys, to recover keys, or both.

4. Choose the statsu of requests you want to see by selecting one of the following choices from the “Request status” pull-down menu:

   - **Show canceled requests.** Unless your system is specially configured for it, there will be no cancelled requests.
   - **Show rejected requests.** Rejected requests do not comply with your company’s archival or recovery policies. Unless your system is specially configured for it, there will be no rejected requests.
   - **Show completed requests.** Completed requests include archival requests for which proof of archival has been sent and completed recovery requests.
   - **Show all requests.** All requests stored in the system.

5. To start the list at a specific place in the queue, enter the starting request identifier in decimal or hexadecimal form.

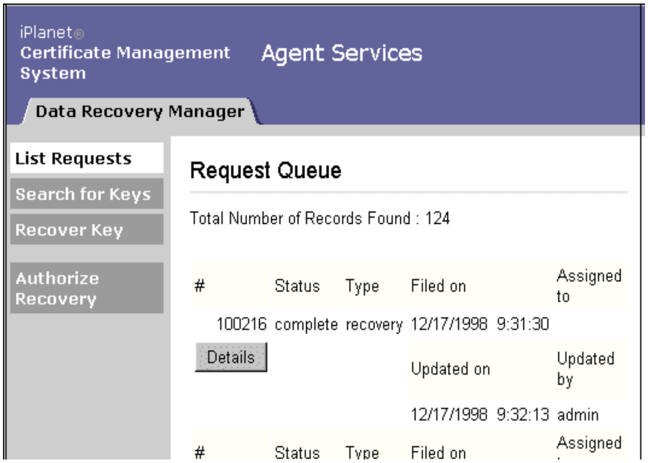
   Use `0x` to indicate the beginning of a hexadecimal number; for example, `0x2A`. (Key identifiers are displayed in hexadecimal form in the Search Results and Details pages.)

6. Choose the number of matching requests you want to see.

   When you specify a number *n*, the system displays the first *n* requests after the starting request identifier that match your specified criteria.

7. Click Find.

   The Data Recovery Manager displays a list of the key service requests that match your search criteria. You can select a request in the list and examine it in more detail. For instructions, see “Selecting a Key” on page 68.



Request Queue

Total Number of Records Found : 124

#	Status	Type	Filed on	Assigned to
100216	complete	recovery	12/17/1998 9:31:30	
			Updated on	Updated by
			12/17/1998 9:32:13	admin
#	Status	Type	Filed on	Assigned

Selecting a Request

To select a request from the queue:

1. On the Data Recovery Manager’s Agent Services page, click List Requests, specify search criteria, and click Find to display a list of key service requests.

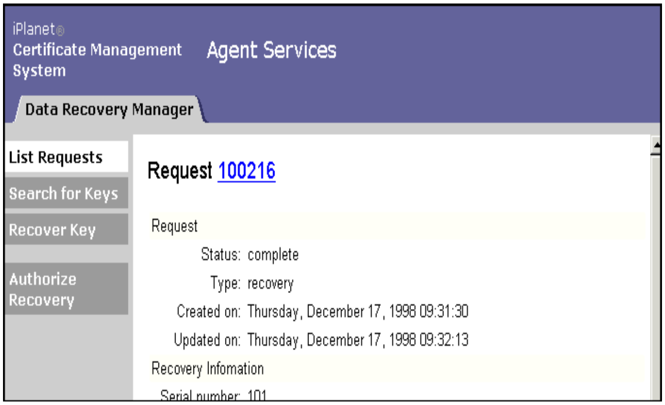
   For details, see “Listing Key Service Requests” on page 73.

2. On the Key Service Request Queue form, find a particular request.

   If the request you want to see is not shown, scroll to the bottom of the list and select the Next or Previous group of requests.

3. Click Details next to the selected request.

   The details of the selected key service request appear in the Request details form. You cannot manipulate the request in any way.



Request 100216

Request

Status: complete

Type: recovery

Created on: Thursday, December 17, 1998 09:31:30

Updated on: Thursday, December 17, 1998 09:32:13

Recovery Infomation

Serial number: 101

If the system changes the state of the displayed request, and if you use your browser's Back or Forward buttons or the Go (history) menu to move to another page, the data shown can become out of date. To refresh the data, click the highlighted key identifier at the top of the page.

Chapter 6

Managing OCSP Service Related Tasks

This chapter describes how to perform Online Certificate Status Manager agent's tasks, such as identifying a CA to the Online Certificate Status Manager, adding a CRL to the Online Certificate Status Manager's internal datbase and so on. This service is available only when the Online Certificate Status Manager subsystem is installed. The Online Certificate Status Manager Agent Services page allows certified agents to accomplish these tasks.

This chapter has the following sections:

Listing CAs Identified by Online Certificate Status Manager

The Online Certificate Status Manager can be configured to receive CRLs from multiple Certificate Managers. Each Certificate Manager that can publish CRLs to the Online Certificate Status Manager must have its *CA signing certificate* stored in the internal database of the Online Certificate Status Manager. For instructions, see "Identifying a CA to Online Certificate Status Manager" on page 78.

At any given time, you can see the list Certificate Managers that are currently recognized by the Online Certificate Status Manager.

To see the list of Certificate Managers:

1. Open a web browser window.
2. Go to the Online Certificate Status Manager's Agent interface. The URL is in this format: `https://<hostname>:<port>`.

   The Online Certificate Status Manager Agent Services interface appears.
3. In the left frame, click List Certificate Authorities.

   The resulting form should show information about the Certificate Managers (CAs) that are recognized by the Online Certificate Status Manager.

Identifying a CA to Online Certificate Status Manager

The Online Certificate Status Manager can be configured to receive CRLs from multiple Certificate Managers. Before you configure a Certificate Manager to publish CRLs to the Online Certificate Status Manager, you must identify the Certificate Manager to the Online Certificate Status Manager. You do this by storing the Certificate Manager's *CA signing certificate* in the internal database of the Online Certificate Status Manager.

The steps below explain how to store the Certificate Manager's *CA signing certificate* in the internal database of the Online Certificate Status Manager:

1. Open a web browser window.
2. Go the Certificate Manager's end-entity interface. The URL is in `https://<hostname>:<SSL_port>` or `http://<hostname>:<port>` format.
3. Select the Retrieval tab, and in the left frame, click List Certificates.
4. In the resulting form, click List.

   A list of certificates appear.
5. Locate the Certificate Manager's CA signing certificate by looking at the subject name of the certificate.

   Typically, the CA signing certificate is the first certificate the Certificate Manager issues.
6. Click Details.

7. In the resulting page, scroll to the section that says “Base 64 encoded certificate” and shows the CA signing certificate in its base-64 encoded format.

8. Copy the base-64 encoded certificate, including the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` marker lines, to the clipboard or a text file.

   The copied information should look similar to the following example:

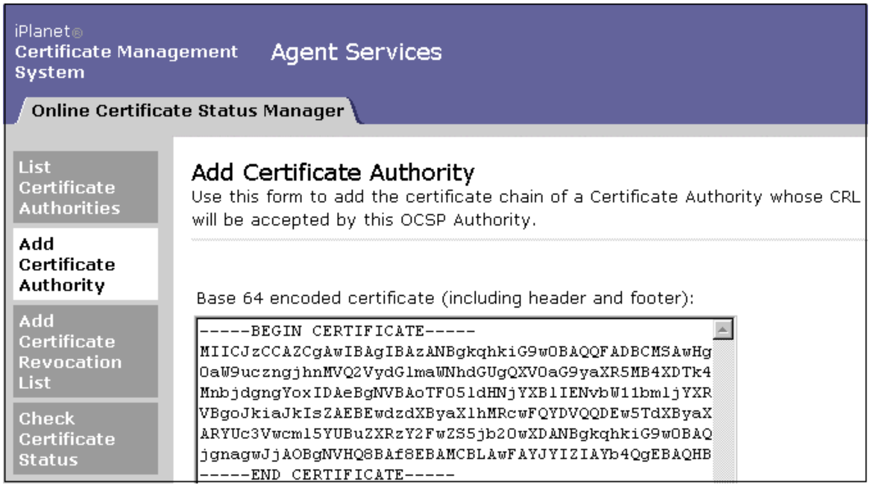
```
-----BEGIN CERTIFICATE-----

MIICJzCCAZCgAwIBAgIBAzANBgkqhkiG9w0BAQQFADBCMSAwHgYDVQQKExdOZXR
Y2FwZSBDb21tdW5pYF0aW9ucznjhnMVQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X
DTk4MDgyNzE5MDAwMFoXDTk5MDIyMzE5MDAwMnbjdgngYoxIDAeBgNVBAoTF05ld
HNjYXBlIENvbW11bmljYXRpb25zMQ8wDQYDVQQLEwZQZW9wbGUxFzAVBgoJkiaJk
IsZAEBEwdzdXByaXlhMRcwFQYDVQQDEw5TdXByaXlhIFNoZXR0eTEjMCEGCSqGSI
b3DbndgJARYUc3Vwcml5YUBuZXRzY2FwZS5jb20wXDANBgkqhkiG9w0BAQEFAANL
ADBIAkEAoYiYgthgtbbnjfngjnjgnagwJjAOBgNVHQ8BAf8EBAMCBLAwFAYJYIZI
AYb4QgEBAQHBAQDAgCAMA0GCSqGSIb3DQEBBAUAA

-----END CERTIFICATE-----
```

9. Go to the Online Certificate Status Manager’s Agent interface. The URL is in this format: `https://<hostname>:<port>`.

   The Online Certificate Status Manager Agent Services interface appears.

10. In the left frame, click Add Certificate Authority.

11. In the resulting form, paste the encoded CA signing certificate inside the text area labeled “Base 64 encoded certificate (including header and footer).”



iPlanet®
Certificate Management System
Agent Services
Online Certificate Status Manager
List Certificate Authorities
Add Certificate Authority
Add Certificate Revocation List
Check Certificate Status

Add Certificate Authority

Use this form to add the certificate chain of a Certificate Authority whose CRL will be accepted by this OCSP Authority.

Base 64 encoded certificate (including header and footer):

```
-----BEGIN CERTIFICATE-----
MIICJzCCAZCgAwIBAgIBAzANBgkqhkiG9w0BAQQFADBCMSAwHg
0aW9ucznjhnMVQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4XDTk4
MnbjdgngYoxIDAeBgNVBAoTF05ldHNjYXBlIENvbW11bmljYXR
VBgoJkiaJkIsZAEBEwdzdXByaXlhMRcwFQYDVQQDEw5TdXByaX
ARYUc3Vwcml5YUBuZXRzY2FwZS5jb20wXDANBgkqhkiG9w0BAQ
jgnagwJjAOBgNVHQ8BAf8EBAMCBLAwFAYJYIZIAYb4QgEBAQHB
-----END CERTIFICATE-----
```

12. Click Add.

    The certificate is added to the internal database of the Online Certificate Status Manager.

13. To verify that the certificate is added successfully, in the left frame, click List Certificate Authorities.

    The resulting form should show information about the Certificate Manager (CA) you just added.

Adding a CRL to Online Certificate Status Manager

There may arise a situation when a Certificate Manager is unable to publish its CRL to the Online Certificate Status Manager. In such exigencies, you can manually add a CRL to the internal database of the Online Certificate Status Manager.

To add a CRL to the internal database:

1. Open a web browser window.

2. Go to the Certificate Manager's Agent interface (see "Accessing Agent Services" on page 23). The URL is in this format: `https://<hostname>:<port>`. You must submit the proper client certificate to get access to this page.

   The Certificate Manager Agent Services interface appears.

3. Select the Retrieval tab, and in the left frame, click Import Certificate Revocation List.

4. In the resulting form, select the option to display the CRL in base-64 encoded format and click Submit.

5. In the resulting page, scroll to the section that says "Base-64 encoded CRL" which shows the CRL in its base-64 encoded format.

6. Copy the base-64 encoded CRL, including the `-----BEGIN CRL-----` and `-----END CRL-----` marker lines, to the clipboard or a text file.

   The copied information should look similar to the following example:

```
-----BEGIN CRL-----

MIICJzCCAZCgAwIBAgIBAzANBgkqhkiG9w0BAQQFADBCMSAwHgYDVQQKExdOZXRz
Y2FwZSBDb21tdW5pYF0aW9uczngjhnMVQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X
DTk4MDgyNzE5MDAwMFoXDTk5MDIyMzE5MDAwMnbjdgngYoxIDAeBgNVBAoTF05ld
HNjYXBlIENvbW11bmljYXRpb25zMQ8wDQYDVQQLEwZQZW9wbGUxFzAVBgoJkiaJk
IsZAEBEwdzdXByaXlhMRcwFQYDVQQDEw5TdXByaXlhIFNoZXR0eTEjMCEGCSqGSI
b3DbndgJARYUc3Vwcml5YUBuZXRzY2FwZS5jb20wXDANBgkqhkiG9w0BAQEFAANL
ADBIAkEAoYiYgthgtbbnjfngjnjgnagwJjAOBgNVHQ8BAf8EBAMCBLAwFAYJYIZI
AYb4QgEBAQHBAQDAgCAMA0GCSqGSIb3DQEBBAUAA4GBAFi9FzyJlLmS+kzsue0kT
XawbwamGdYql2w4hIBgdR+jWeLmD4CP4xzmKdvQ6IqD2q8DBs9lRQu9JYg129o

-----END CRL-----
```

7. Go to the Online Certificate Status Manager's Agent interface. The URL is in this format: `https://<hostname>:<port>`.

   The Online Certificate Status Manager Agent Services interface appears.

8. In the left frame, click Add Certificate Revocation List.

9. In the resulting form, paste the encoded CRL inside the text area labeled "Base 64 encoded certificate revocation list (including the header and footer)."

10. Click Add.

    The CRL is added to the internal database of the Online Certificate Status Manager.

Checking the Revocation Status of a Certificate

You can check the revocation status of a certificate by submitting the certificate in its base-64 encoded format to the Online Certificate Status Manager:

1. Copy the base-64 encoded certificate, including the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` marker lines, to the clipboard or a text file.

   The copied information should look similar to the following example:

```
-----BEGIN CERTIFICATE-----

MIICJzCCAZCgAwIBAgIByrgrugrwuguvgrvhfeygyDBCMSAwHgYDVQQKExdOZXRz
Y2FwZSBDb21tdW5pYFdih9ucznjhnMVQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X
DTk4MDgyNzE5MDAwMFoXDTk5MDIyMzE5MDAwMnbjdgngYoxIDAeBgNVBAoTF05ld
HNjYXBlafkhbfgsdbutihdhb25zMQ8wDQYDVQQLEwZQZW9wbGUxFzAVBgoJkiaJk
IsZAEBEwdzdXByaXlhMRcwFQYDVQQDEw5TdXByaXlhIFNoZXR0eTEjMCEGCSqGSI
b3DbndgJASdUc3Vwcml5YUBuZXRzY2FwZS5jb20wXDANBgkqhkiG9w0BAQEFAANL
ADBIAkEAoYiYgthgtbbnjfngjnjgnagwJjAOBgNVHQ8BAf8EBAMCBLAwFAYJYIZI
AYb4QgEBAQHBAQDAgCAMA0GCSqGSIb3DQEBBAUAA

-----END CERTIFICATE-----
```

2. Go to the Online Certificate Status Manager Agent Services page (see “Accessing Agent Services” on page 23).

   You must submit the proper client certificate to get access to this page.

3. In the left frame, click Check Certificate Status.

4. In the resulting form, paste the certificate inside the text area labeled “Base 64 encoded certificate.”

5. Click Check.

   The resulting form should inform you about the status of the certificate you just submitted.

Index