HITACHI
Inspire the Next

Hitachi Encrypted Communications User's Guide

Hitachi Universal Storage Platform V
Hitachi Universal Storage Platform VM
Hitachi TagmaStore® Universal Storage Platform
Hitachi TagmaStore® Network Storage Controller
Hitachi Lightning 9900™ V Series

FastFind Links

Hitachi Data Systems

MK-96RD631-04

Contents

Preface

This document describes and provides instructions for using SSL encrypted communication with the Storage Navigator software for the following Hitachi storage systems: Hitachi Universal Storage Platform V and Universal Storage Platform VM (USP V/VM), Hitachi TagmaStore® Universal Storage Platform and Network Storage Controller (USP/NSC), and Hitachi Lightning 9900™ V Series.

Please read this document carefully to understand how to use this product, and maintain a copy for reference purposes.

This preface includes the following information:

Intended Audience

This document is intended for system administrators, Hitachi Data Systems representatives, and authorized service providers who are involved in installing, configuring, and operating Hitachi storage systems and software.

This document assumes the following:

- The user has a background in data processing and understands RAID storage systems and their basic functions.
- The user is familiar with the Hitachi storage system and has read the *User and Reference Guide* for the storage system.
- The user has read and understands the *Storage Navigator User's Guide* for the storage system.
- The user is familiar with the operating system and web browser software on the system hosting the Storage Navigator software. For details on the applicable operating systems and web browser software, please refer to *Storage Navigator User's Guide* for the storage system.

Note for USP V/VM and USP/NSC Users Only: There are different types of users for USP V/VM and USP/NSC: storage administrators and storage partition administrators. The functions described in this manual are not for the storage partition administrators. For details on the user types, please refer to the *Storage Navigator User's Guide* for the storage system.

Product Version

This document revision applies to the following:

- USP V/USP VM microcode version 60-06-0x or later
- TagmaStore USP/NSC microcode version 50-05-0*x-xx*/*xx* or later
- 9900V microcode version 21-10-0*x*/*xx* or later

Document Revision Level

Revision	Date	Description
MK-96RD631-P	February 2007	Preliminary Release
MK-96RD631-00	April 2007	Initial release, supersedes and replaces MK-96RD631-P
MK-96RD631-01	May 2007	Revision 1, supersedes and replaces MK-96RD631-00
MK-96RD631-02	September 2007	Revision 2, supersedes and replaces MK-96RD631-01
MK-96RD631-03	November 2009	Revision 3, supersedes and replaces MK-96RD631-02
MK-96RD631-04	April 2011	Revision 4, supersedes and replaces MK-96RD631-03

Source Documents for this Revision

- Not applicable.

Changes in this Revision

- Updated the procedure for creating a private key (download SSL, not provided on CD-ROM) (Creating a Private Key (.key file)).

Document Organization

The following table provides an overview of the contents and organization of this document. Click the chapter title in the left column to go to that chapter. The first page of each chapter provides links to the sections in that chapter.

Chapter	Description
About Encrypted Communication	Provides and overview of SSL communications.
Using the Encrypted Communications GUI	Provides an overview of the Encrypted Communications GUI including a step-by-step tutorial for updating certificate files.
Performing SSL Operations	This chapter provides a tutorial for performing SSL operations.
Troubleshooting	Troubleshooting

Referenced Documents

Hitachi Universal Storage Platform V/VM:

- *Storage Navigator User's Guide*, MK-96RD621
- *User and Reference Guide*, MK-96RD635

Hitachi TagmaStore USP/NSC:

- *Storage Navigator User's Guide*, MK-94RD206
- *TagmaStore USP User and Reference Guide*, MK-94RD231
- *TagmaStore NSC User and Reference Guide*, MK-95RD279

Hitachi Lightning 9900V:

- *Remote Console – Storage Navigator User's Guide*, MK-92RD101
- *User and Reference Guide*, MK-92RD100

Document Conventions

The term “Hitachi storage system” refers to all models of the following Hitachi storage systems unless otherwise noted: Hitachi Universal Storage Platform V/VM, Hitachi TagmaStore USP/NSC, Hitachi Lightning 9900V.

This document uses the following typographic conventions:

Typographic Convention	Description
Bold	Indicates text on a window, other than the window title, including menus, menu options, buttons, fields, and labels. Example: Click **OK**.
Italic	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: copy *source-file target-file* Angled brackets (< >) are also used to indicate variables.
screen/code	Indicates text that is displayed on screen or entered by the user. Example: `# pairdisplay -g oradb`
< > angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: `# pairdisplay -g <group>` Italic font is also used to indicate variables.
[ ] square brackets	Indicates optional values. Example: [a | b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a | b } indicates that you must choose either a or b.
| vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a | b] indicates that you can choose a, b, or nothing. { a | b } indicates that you must choose either a or b.
underline	Indicates the default value. Example: [a | b]

This document uses the following icons to draw attention to information:

Icon	Meaning	Description
	Note	Calls attention to important and/or additional information.
	Tip	Provides helpful information, guidelines, or suggestions for performing tasks more effectively.
	Caution	Warns the user of adverse conditions and/or consequences (e.g., disruptive operations).
	WARNING	Warns the user of severe conditions and/or consequences (e.g., destructive operations).

Convention for Storage Capacity Values

Physical storage capacity values (e.g., disk drive capacity) are calculated based on the following values:

1 kilobyte (KB) = 1,000 bytes
1 megabyte (MB) = $1,000^2$ bytes
1 gigabyte (GB) = $1,000^3$ bytes
1 terabyte (TB) = $1,000^4$ bytes
1 petabyte (PB) = $1,000^5$ bytes

Logical storage capacity values (e.g., logical device capacity) are calculated based on the following values:

1 KB = 1,024 bytes
1 MB = 1,024 KB or $1,024^2$ bytes
1 GB = 1,024 MB or $1,024^3$ bytes
1 TB = 1,024 GB or $1,024^4$ bytes
1 PB = 1,024 TB or $1,024^5$ bytes
1 block = 512 bytes

Getting Help

If you need to call the Hitachi Data Systems Support Center, please provide as much information about the problem as possible, including:

- The circumstances surrounding the error or failure.
- The content of any error message(s) displayed on the host system(s).
- The content of any error message(s) displayed on Storage Navigator.
- The Storage Navigator configuration information (use the FD Dump Tool).
- The service information messages (SIMs), including reference codes and severity levels, displayed by Storage Navigator.

The Hitachi Data Systems customer support staff is available 24 hours/day, seven days a week. If you need technical support, please call:

- United States: (800) 446-0744
- Outside the United States: (858) 547-4526

Comments

Please send us your comments on this document: doc.comments@hds.com
Include the document title, number, and revision, and refer to specific section(s) and paragraph(s) whenever possible.

Thank you! (All comments become the property of Hitachi Data Systems Corporation.)

1

About Encrypted Communications

In order to improve the security of remote operations from Storage Navigator to a storage system, set up SSL encrypted communication to encrypt your login conversations between client and server computers. The user ID and password required for logging on to Storage Navigator will then be encrypted to ensure a higher level of security.

Secure sockets layer (SSL) is a protocol first developed by Netscape® to securely transmit data over the Internet. Two SSL-enabled peers use their private and public keys to establish a secure communication session, with each peer encrypting transmitted data with a randomly generated and agreed-upon symmetric key.

This document provides the information you need to set up SSL communication on your Storage Navigator computer. Creating keypairs, acquiring a signed certificate, uploading that certificate to the service processor (SVP), setting the web browser to accept certificates, and blocking HTTP communication to the storage system are all covered.

SSL requires that the SVP be set up to use the Apache™ HTTP server. You will need to change the web server (SVP) to Apache as it supports SSL. This will be performed by a Hitachi Data Systems representative.

Server certificates require the use of a host name instead of an IP address when adding or changing a storage device. See the *Storage Navigator User's Guide* for the storage system for more information on adding or changing storage devices.

Important: If you enable SSL, you must make sure that the key pair and associated server certificate do not expire. If either the key pair or the server certificate expires, you will be unable to connect to the SVP.

2

Using the Encrypted Communications GUI

This chapter provides an overview of the Encrypted Communications GUI including instructions for updating certificate files.

Updating Certificate Files Login Dialog Box

Use this dialog box when updating the certificate to enter the administrator user ID and password.

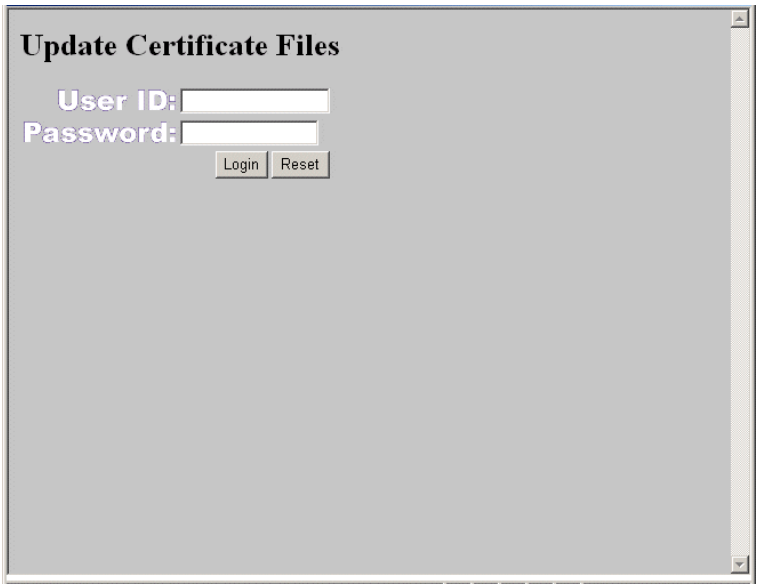

Figure 2-1 Update Certificate Files Login Dialog Box

Update Certificate Files Upload Dialog Box

Use this dialog box to specify and upload certificate files.

This dialog box does not appear if you are using 9900V.

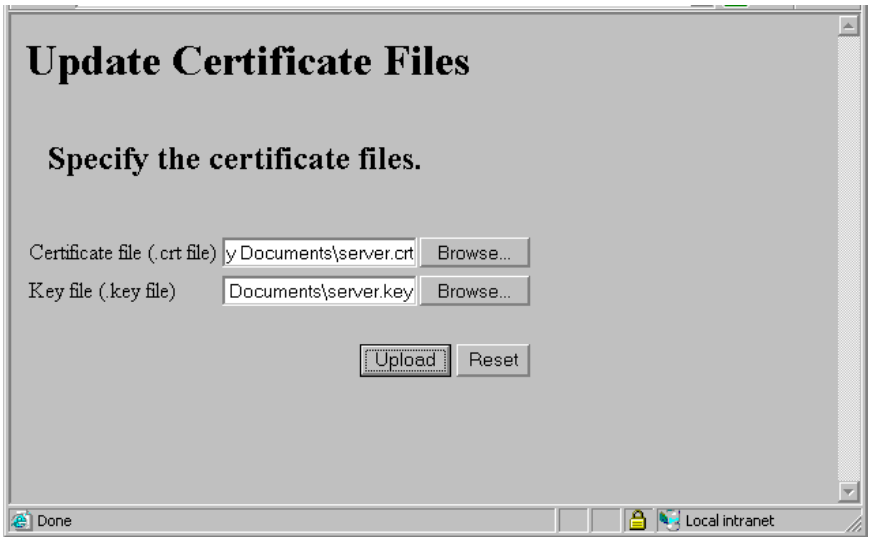

Figure 2-2 Update Certificate Files Dialog Box

Item	Description
Certificate file (.crt file)	Enter the full pathname and file name in the text box, or click **Browse** and select the certificate file in the file selection dialog box.
Key file (.key file)	Enter the full pathname and file name in the text box, or click **Browse** and select the key file in the file selection dialog box.
Upload	After entering the pathname and file name, click to upload the certificate files.
Reset	Reset the information in the dialog box.

3

Performing SSL Operations

This chapter provides a tutorial for performing SSL operations.

- ☐ Creating a Keypair
- ☐ Acquiring a Signed Certificate
- ☐ Uploading the Signed Certificate to the SVP
- ☐ Setting the Web Browser to Accept Self-signed Certificates
- ☐ Blocking HTTP Communications to the Storage System

Creating a Keypair

To enable SSL, you need to create a keypair (public and private key). A keypair is two mathematically-related cryptographic keys consisting of a private key and its associated public key.

- ☐ Creating a Private Key (.key file)
- ☐ Creating a Public Key (.csr file)

These instructions use Windows® 2000 as an example.

If you are using Solaris™ or HP-UX®, download software for creating a keypair such as OpenSSL (http://www.openssl.org/), and follow the manufacturer's instructions.

The program (openssl.exe) for creating private and public keys is available on the CD for SSL communication provided with this product.

Creating a Private Key (.key file)

To create a private key:

1. Download software for creating a keypair, such as OpenSSL (http://www.openssl.org/), and follow the manufacturer's instructions.
2. Open a command prompt.
3. Navigate to the directory where you installed OpenSSL (e.g., `C:\openssl`), and execute the following command:

   ```
   C:\openssl> openssl genrsa -out server.key 1024
   ```

   This creates a file called **server.key** in the **openssl** folder. This file becomes the private key.

Creating a Public Key (.csr file)

To create a public key:

1. Open a command prompt, navigate to the directory where you installed OpenSSL (e.g., `C:\openssl`), and execute the following command:

   ```
   C:\openssl> openssl req -new -key server.key -config openssl.cnf
   -out server.csr
   ```

   When this command is executed, MD5 is used for the hush algorithm. If you want to use SHA-1 for the hush algorithm, execute the following command:

   ```
   C:\openssl> openssl req –sha1 -new -key server.key -config
   openssl.cnf -out server.csr
   ```

2. Enter the following information (Figure 3-1 is an example; enter your own information):
   - Country Name (2 letter code)
   - State or Province Name
   - Locality Name (e.g., city)
   - Organization Name (e.g., company)
   - Organization Unit Name (e.g., department name)
   - Common Name: If you are going to create a self-signed certificate, enter the IP address of the web server (SVP). If you are going to obtain a signed and trusted certificate, the server name must be the same as the host name of the storage device. See the *Storage Navigator User's Guide* for more information on adding or changing storage devices.
   - Email Address: (not entered in the example)
   - Challenge password (optional)
   - Company name (optional)

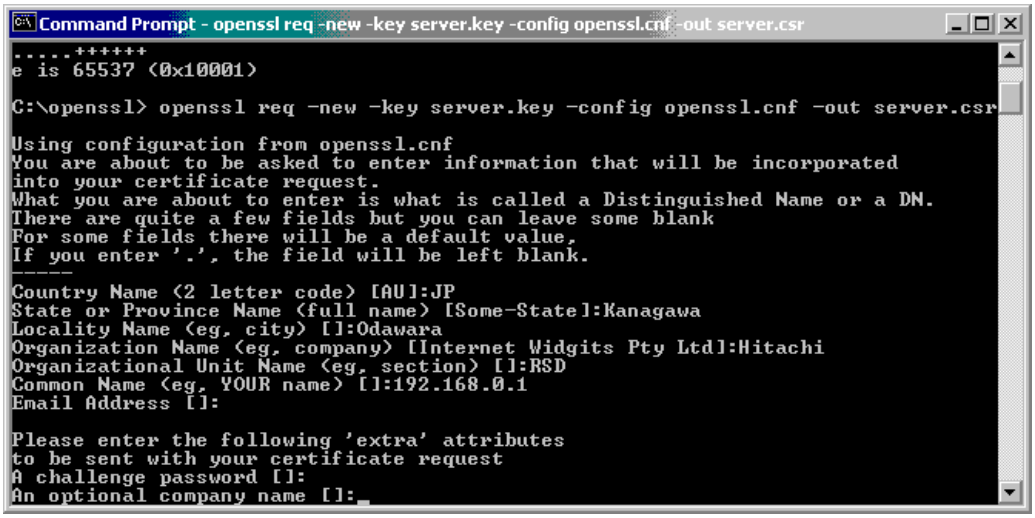

Figure 3-1 Creating a Public Key

Acquiring a Signed Certificate

A server certificate (sometimes also called a digital certificate) forms an association between an identity (in this case the SVP server) and a specific keypair. A server certificate is used to identify the SVP server to a client so that the server and client can communicate using SSL.

Server certificates come in two basic types:

- **Self-signed:** This is the case where you generate your own certificate, so that the subject of the certificate is the same as the issuer of the certificate. If the communication between Storage Navigator computers and the SVP is on an internal LAN behind a firewall, you may find that this option provides sufficient security. See Creating a Self-Signed Certificate for more information.
- **Signed and Trusted:** When a Certificate Signing Request (CSR) is generated and sent to a well-known and trusted Certificate Authority (CA) for signing, and is then signed and returned by the Certificate Authority, your certificate is considered signed and trusted. One such Certificate Authority is VeriSign® (http://www.verisign.com/). See Creating a Signed and Trusted Certificate for more information . Using signed and trusted certificates adds extra cost and requirements.

Creating a Self-Signed Certificate

To create a self-signed certificate, open a command prompt, navigate to the directory where you installed OpenSSL (e.g., `C:\openssl`), and execute the following command:

```
C:\openssl> openssl x509 -req -days 10000 -in server.csr -signkey
server.key -out server.crt
```

When this command is executed, MD5 is used for the hush algorithm. If you want to use SHA-1 for the hush algorithm, execute the following command:

```
C:\openssl> openssl x509 -req –sha1 -days 10000 -in server.csr
-signkey server.key -out server.crt
```

This creates a **server.crt** file in the **openssl** folder, which is valid for 10,000 days. This is the signed private key, which is also referred to as a self-signed certificate.

Creating a Signed and Trusted Certificate

If you want to create a signed and trusted certificate, you need to create a certificate signing request (CSR), send that file to a Certificate Authority (CA), and request that the CA issue a signed and trusted certificate. Each certificate authority has its own procedures and requirements, and there is generally a cost for doing so. The signed and trusted certificate is the signed public key.

Uploading the Signed Certificate to the SVP

In order to use SSL-encrypted communication, you need to update and upload both the private key and the signed server certificate (public key) to the web server (SVP).

- ☐ Instructions for USP V/VM
- ☐ Instructions for USP/NSC
- ☐ Instructions for 9900V

Instructions for USP V/VM

To update and upload a signed certificate:

1. Log off of all Storage Navigator computers attached to the SVP.
2. Start both the Storage Navigator computer and your web browser.
3. To open the Update Certificate Files logon dialog box, specify the following URL:

   `http://xxx.xxx.xxx.xxx/cgi-bin/utility/toolpanel.cgi`

   where *xxx.xxx.xxx.xxx* is the IP address or host name of the SVP.
4. On the **Tool Panel** dialog box (Figure 3-2), select **Update Certificate Files**.
5. If the SVP supports SSL encrypted communication, the **Security Alert** dialog box (Figure 3-3) opens. Click **OK**.
6. The **Security Alert** dialog box for the certificate (Figure 3-4) may also appear. In this case, click **View Certificate**, confirm the certificate is correct, and click **Yes**.
7. On the login dialog box for **Update Certificate Files,** type your Administrator user ID and password and click **Login** (Updating Certificate Files Login Dialog Box).
8. The upload dialog box for **Update Certificate Files** opens (Figure 2-2). Enter both the public key certificate file name in the **Certificate file (.crt file)** box and the private key certificate file name in the private **Key file (.key file)** box. You can enter the file names directly or by clicking **Browse**.
9. Click **Upload** on the upload dialog box of **Update Certificate Files**.
10. On the execution of **Update Certificate Files** confirmation dialog box, (Figure 3-5). click **OK**. The certificate update begins.
11. When the update is complete, the web server restarts and a dialog box (Figure 3-6) appears confirming the restart. Click **OK**.
12. The **Security Alert** dialog box for the certificate (Figure 3-4) may appear. In this case, click **View Certificate** to confirm that the certificate is correct, and click **Yes**.

If an error occurs during the certificate update, an error message will appear (Figure 3-7). Solve the problem, and restart from the logging in to the **Update Certificate Files**.

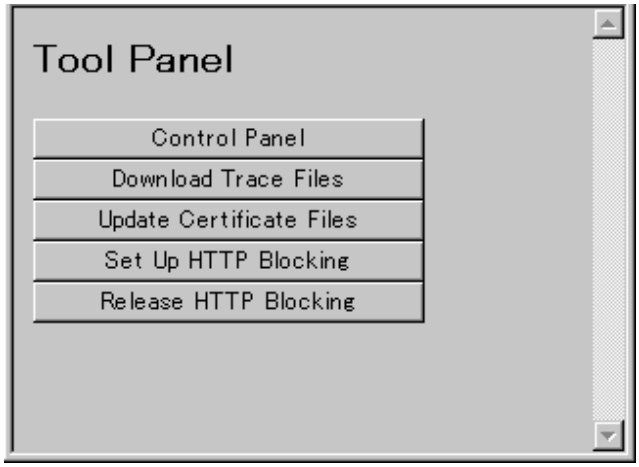

Figure 3-2 Tool Panel Dialog box

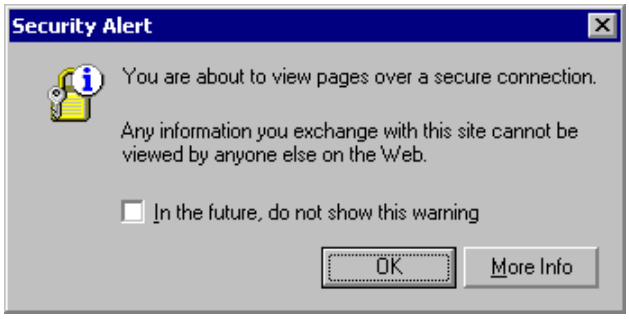

Figure 3-3 Security Alert Dialog Box

Figure 3-4 Security Alert Dialog Box for the Certificate (Displayed Statements and Icons may be Different)

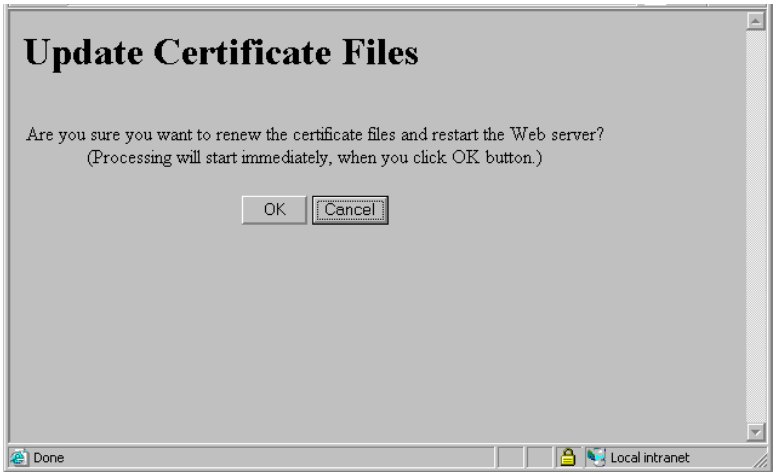

Figure 3-5 Execution of Update Certificate Files Confirmation Dialog Box.

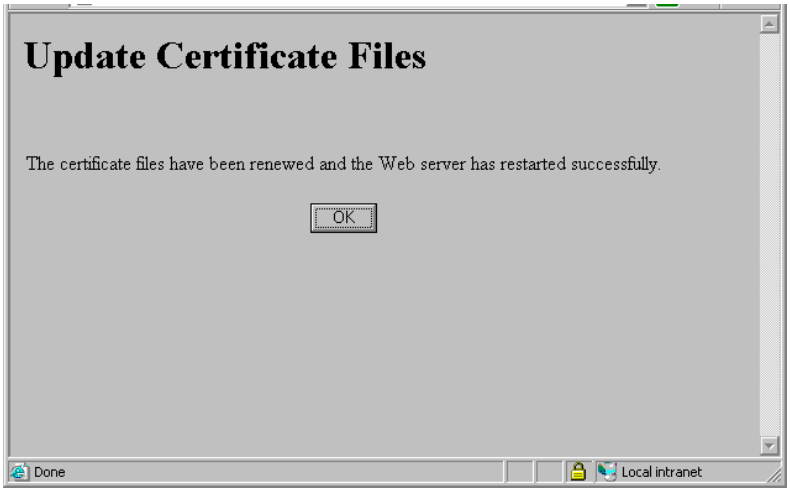

Figure 3-6 Certificate Files Update Completion Dialog Box

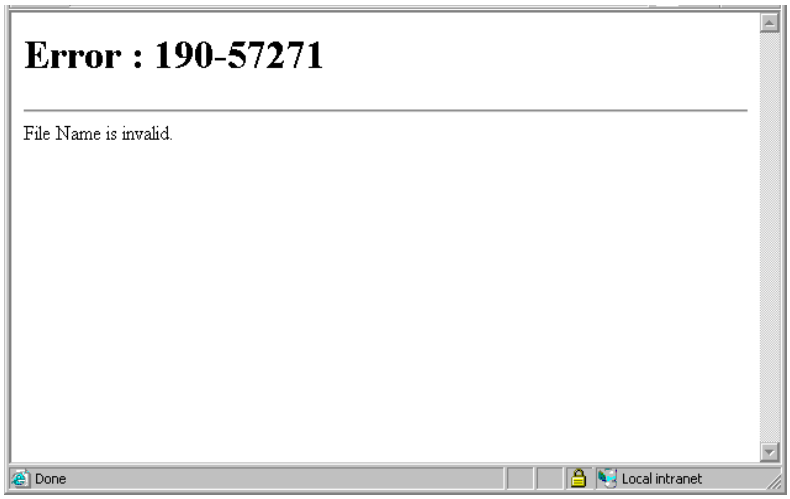

Figure 3-7 Update Certificate Files Error Message Dialog Box

Instructions for USP/NSC

To update and upload a signed certificate:

1. Log off of all Storage Navigator computers attached to the SVP.
2. Start both the Storage Navigator computer and your web browser.
3. To open the Update Certificate Files login dialog box, specify the following URL:

   http://*xxx.xxx.xxx.xxx*/cgi-bin/utility/ssc0000.cgi

   where *xxx.xxx.xxx.xxx* is the IP address or host name of the SVP.
4. If the SVP supports SSL encrypted communication, the Security Alert dialog box (Figure 3-8) opens. Click **OK**.. The Security Alert Certificate (Figure 3-9) may also display. If it does, click **View Certificate** to confirm that the certificate is correct, then click **Yes**.
5. On the login dialog box for Update Certificate Files, type your Administrator User ID, Password, and click **Logon.**
6. On the **Update Certificate Files** dialog box (Figure 2-2), enter both the public key certificate file name in the **Certificate file (.crt file)** box and the private key certificate file name in the **Key file (.key file)** box. You can either type the file names directly or click **Browse** to select the file.
7. If the file names are correct, click **Upload**.
8. On the Update Certificate Files Confirmation dialog box (Figure 3-10), click **OK**.
9. The certificate update begins. When complete, the web server restarts and a dialog box (Figure 3-11) appears to confirm the restart. Click **OK**.

   If an error occurs during the certificate update, an error message will appear (Figure 3-12). Solve the problem and restart the process.

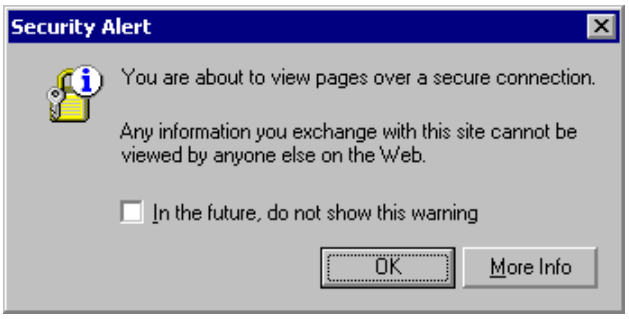

Figure 3-8 Security Alert Dialog Box

Figure 3-9 Security Alert Dialog Box for the Certificate (Displayed Statements and Icons may be Different)

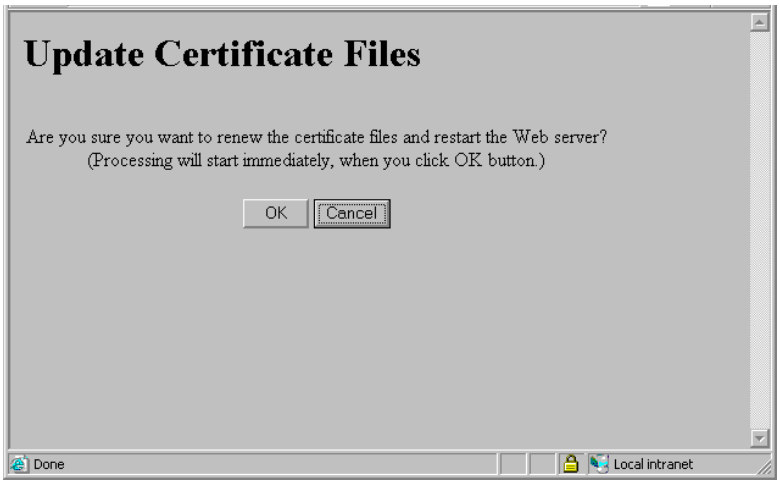

Figure 3-10 Update Certificate Files Confirmation Dialog Box

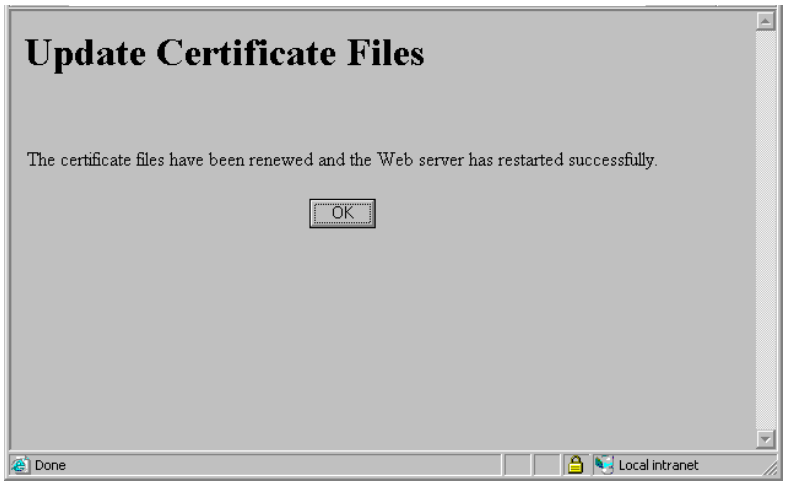

Figure 3-11 Update Certificate Files Completion Dialog Box

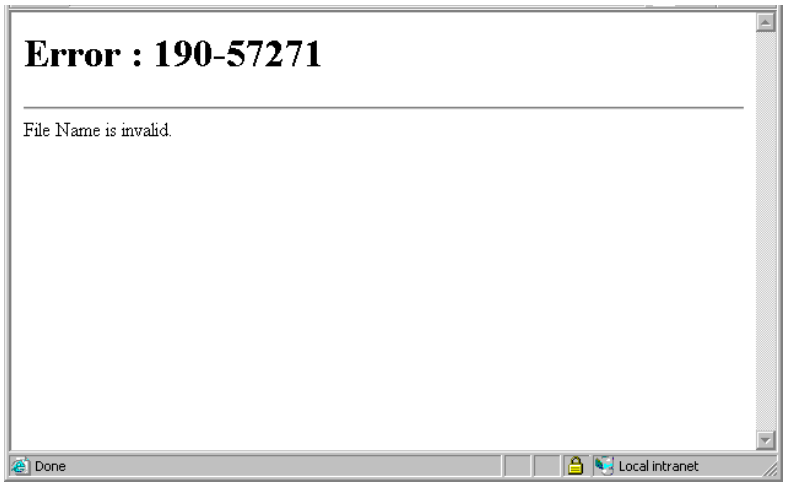

Figure 3-12 Update Certificate Files Error Message Dialog Box

Instructions for 9900V

To update and upload a signed certificate:

1. Download the FTP Client for Storage Navigator.

   For detailed information about the FTP Client, please refer to *9900V Remote Console - Storage Navigator User's Guide*.

2. Log off of all Storage Navigator computers attached to the SVP.
3. Upload the private key (.key file) and the signed server certificate (public key) (.crt file) to the web server (SVP) using the **FTP Client**. Select **AsciiMode** on the upload dialog box as the mode for uploading.
4. Start both the Storage Navigator system and your web browser.
5. To open the Update Certificate Files login dialog box, specify the following URL:

   http://xxx.xxx.xxx.xxx/cgi-bin/utility/ssc0000.cgi

   where xxx.xxx.xxx.xxx is the IP address or host name of the SVP.

6. If the SVP supports SSL encrypted communication, the Security Alert dialog box (Figure 3-13) opens. Click **OK**.
7. The Security Alert Certificate (Figure 3-14) may also appear. If it does, click **View Certificate** to confirm that the certificate is correct, then click **Yes**.
8. On the login dialog box for Update Certificate Files, type your Administrator user ID, password, and click **Logon**.
9. On the confirmation dialog box, click **OK**.
10. The certificate update begins. Once complete, the web server restarts and a dialog box (Figure 3-16) opens confirming the restart. Click **OK**.

    If an error occurs during the certificate update, an error message will appear (Figure 3-17). Solve the problem and restart the process.

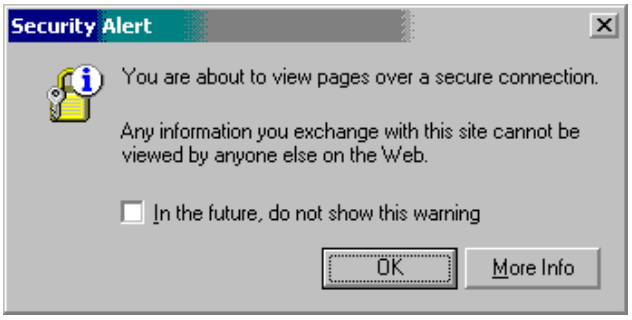

Figure 3-13 Security Alert Dialog Box

Figure 3-14 Security Alert Dialog Box for the Certificate (Displayed Statements and Icons may be Different)

Figure 3-15 Update Certificate Files Confirmation Dialog Box

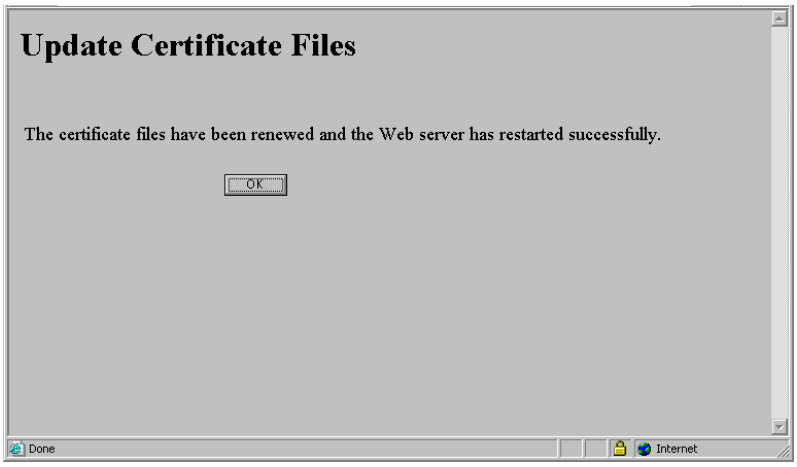

Figure 3-16 Update Certificate Files Completed Dialog Box

Figure 3-17 Update Certificate Files Error Message Dialog Box

Setting the Web Browser to Accept Self-signed Certificates

If using a self-signed certificate, the web browser will display a warning message when it connects to an SSL-enabled SVP. To avoid this message, import the certificate to the web browser.

These sample instructions assume the use of Internet Explorer® 6.0.

To import the certificate to the web browser:

1. Log on to the Storage Navigator using a secure connection (specify the URL using **https**).
2. On the **Security Alert** dialog box (Figure 3-18), click **View Certificate**.
3. On the **Certificate** dialog box (Figure 3-19), click the **General** tab and then click **Install Certificate (I)**.
4. On the **Certificate Import Wizard** (Figure 3-20), click **Next**.
5. On the next screen of the **Certificate Import Wizard** (Figure 3-21), click **Automatically select the certificate store based on the type of certificate** and click **Next**.
6. On the **Certificate Import Wizard** (Completing the Certificate Import Wizard) (Figure 3-22), click **Finish**.
7. On the **Root Certificate Store** dialog box (Figure 3-23), click **Yes**.
8. On the **Certificate Import Wizard** (**Completing the import**) (Figure 3-24), click **OK**.

   You are returned to the **Security Alert** dialog box displayed in the first step (Figure 3-18). Importing the certificate to the Web browser is complete.
9. On the **Security Alert** dialog box, click **Yes**.

Figure 3-18 Security Alert Dialog Box for the certificate (displayed statements and icons may be different)

Figure 3-19 Certificate Dialog Box (Example)

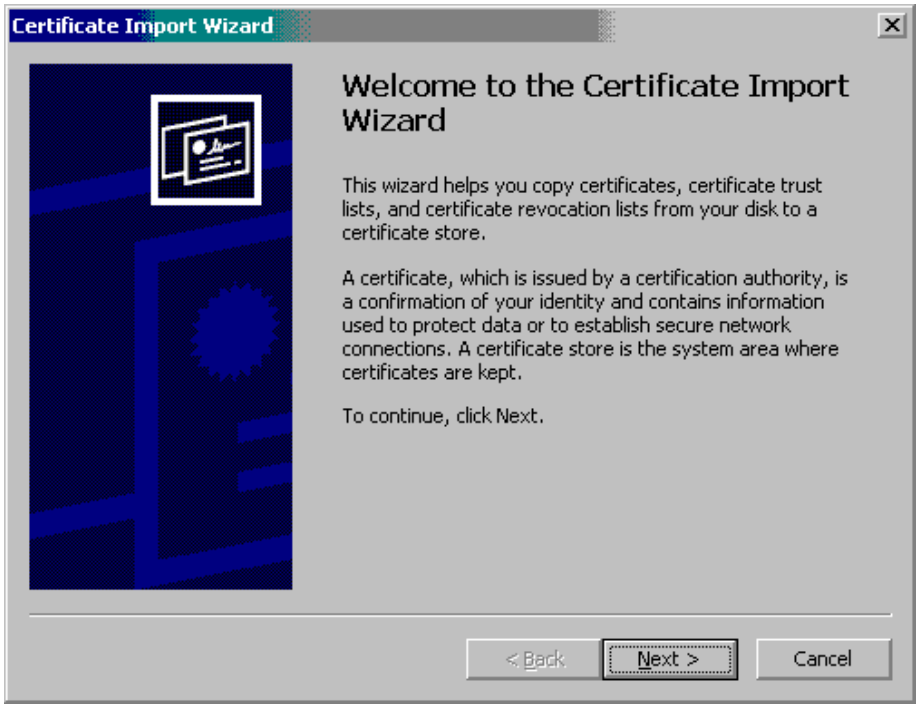

Figure 3-20 Certificate Import Wizard Dialog Box (Welcome to the Certificate Import Wizard)

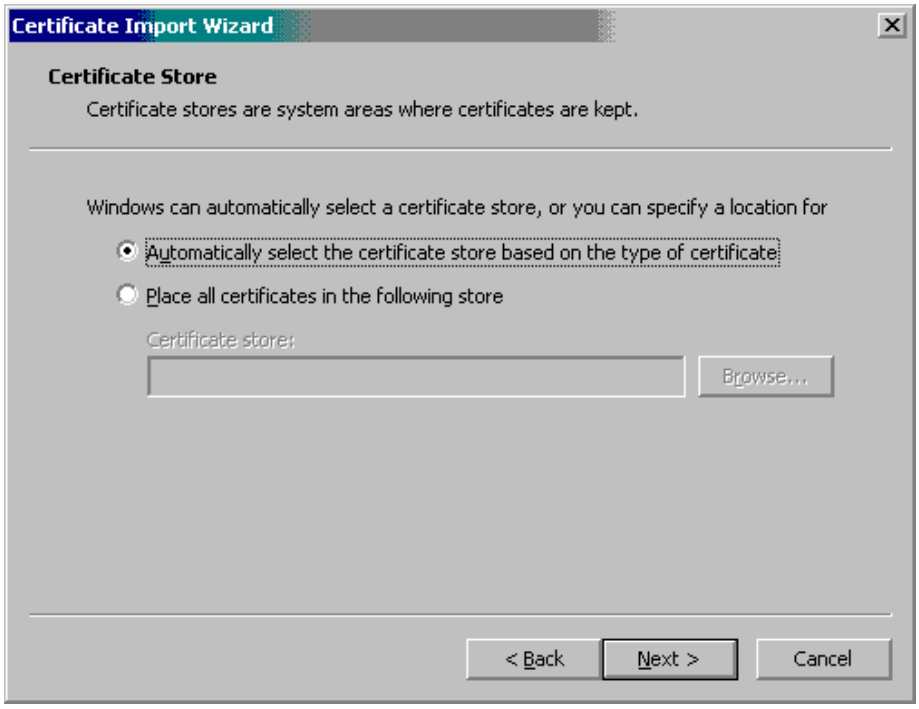

Figure 3-21 Certificate Import Wizard Dialog Box (Certificate Store)

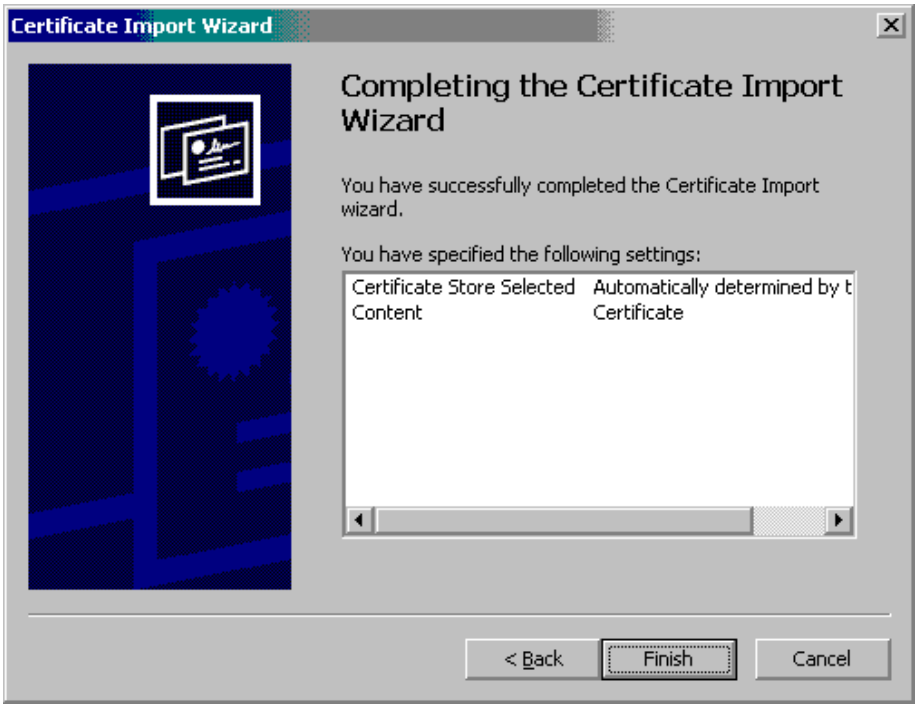

Figure 3-22 Certificate Import Wizard Dialog Box (Completing the Certificate Import Wizard)

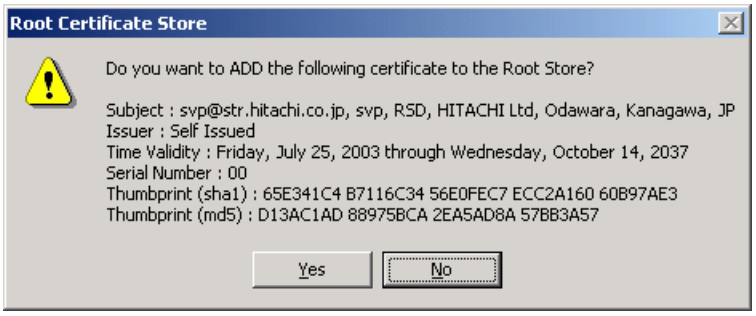

Figure 3-23 Root Certificate Store Dialog Box (Example)

Figure 3-24 Certificate Import Wizard Dialog Box (Completing the import)

Blocking HTTP Communications to the Storage System

If the web server (SVP) supports SSL (HTTPS), use the HTTP setting tool to block access to port 80. In that case, the connection between Storage Navigator and the web server (SVP) will take place on port 443 (HTTPS).

- ☐ Setting Up HTTP Communication Blocking
- ☐ Releasing HTTP Communication Blocking
- ☐ Editing the Storage Device List

If you are using 9900V, you do not need to perform operations explained in this section.

If you are using HiCommand programs to access Storage Navigator, blocking HTTP communication might interfere with that access. Make sure the HiCommand programs can use SSL communication to connect to the Storage Navigator.

Setting Up HTTP Communication Blocking

To set up HTTP communication blocking:

1. Log off all Storage Navigator computers connected to the web server (SVP).
2. Start both the Storage Navigator computer and your web browser.
3. If you are using TagmaStore USP or NSC, point your web browser to the following URL:

   `https://xxx.xxx.xxx.xxx/cgi-bin/utility/sjcp80blk.cgi`

   where *xxx.xxx.xxx.xxx* is the IP address or host name of the SVP.

   If you are using USP V/VM:

   a. Point your web browser to the following URL:

      `https://xxx.xxx.xxx.xxx/cgi-bin/utility/toolpanel.cgi`

      where *xxx.xxx.xxx.xxx* is the IP address or host name of the SVP.

   b. On the **Tool Panel** dialog box (Figure 3-25), click **Set up HTTP Blocking**.
4. Type the User ID and Password for the root storage administrator, then click **Logon** (Figure 3-26).
5. On the **Set up HTTP Blocking** dialog box (Figure 3-27), click **OK**.
6. On the confirmation dialog box (Figure 3-28), click **OK** to implement HTTP blocking. When the configuration change is complete, the SVP will reboot.
7. When the reboot is complete, the HTTP Communications Blocked dialog box appears (Figure 3-29). Click **OK.** You will return to the logon dialog box.

If an error occurs during the operation, an error message will appear (Figure 3-30). Solve the problem and restart the process.

After setting up HTTP communication blocking, the configuration of the Storage Device List must be changed (see Editing the Storage Device List).

You can open the Storage Device List dialog box on your web browser by accessing the following URL:

`https://xxx.xxx.xxx.xxx/cgi-bin/utility/sjc0000.cgi`

where *xxx.xxx.xxx.xxx* is the IP address or the host name of the SVP.

Note: If you have set up HTTP communication blocking, make sure to connect to the Storage Device List dialog box via HTTPS communication.

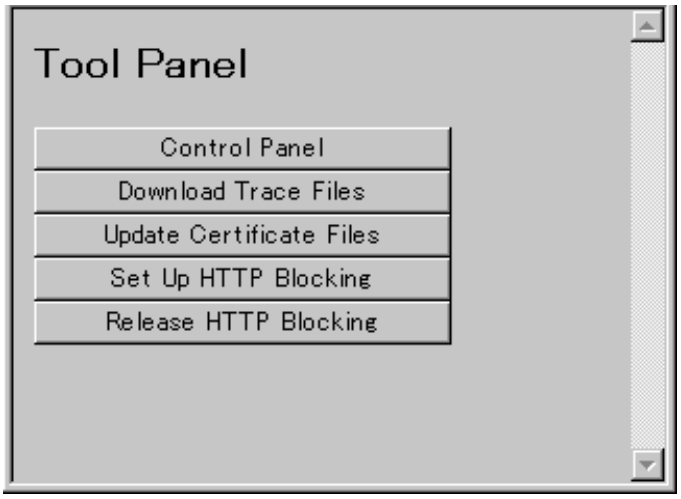

Figure 3-25 Tool Panel Dialog Box

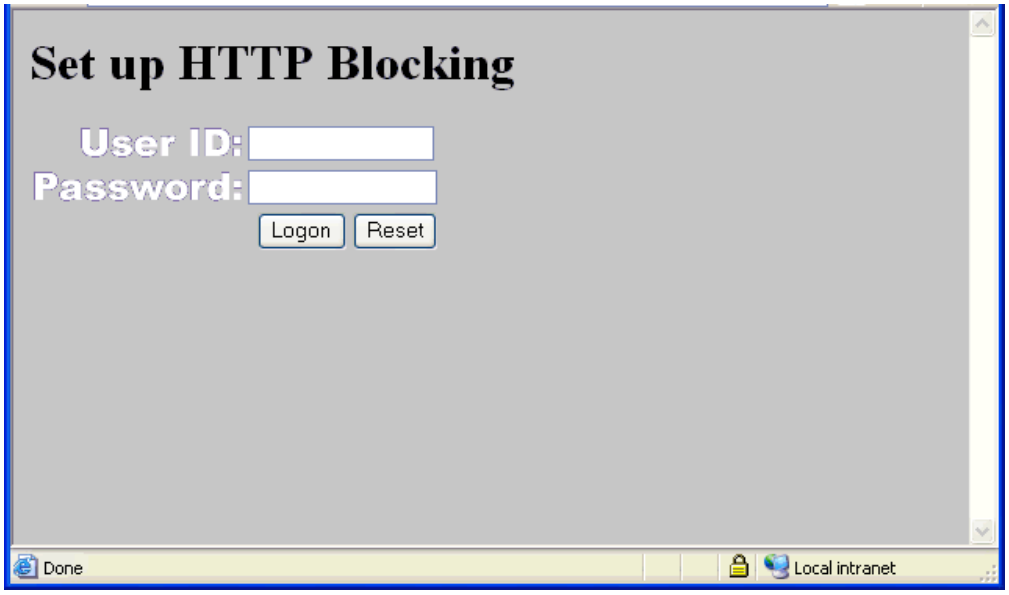

Figure 3-26 Set Up HTTP Blocking Logon Dialog Box

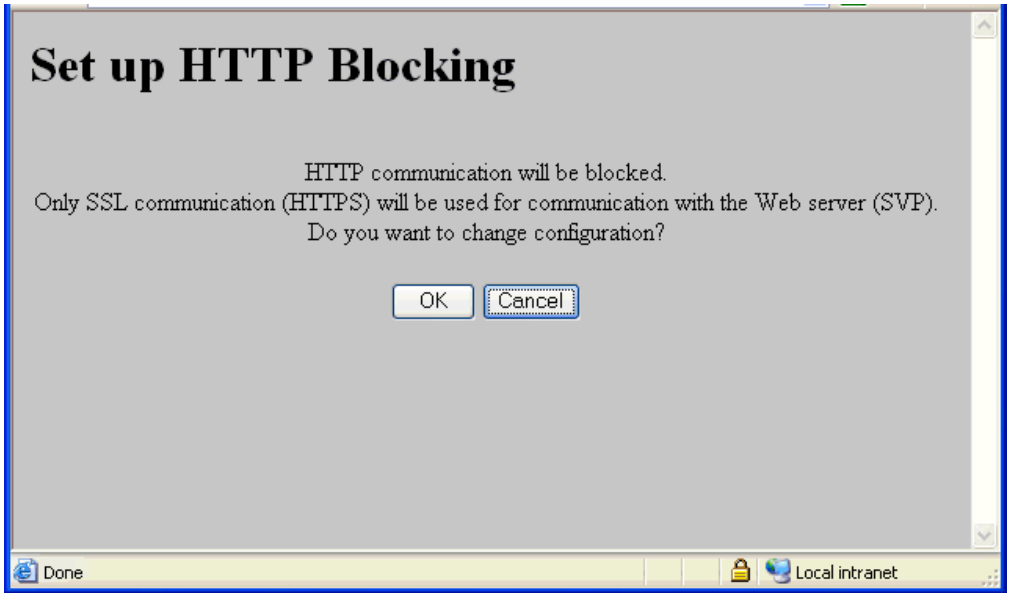

Figure 3-27 Changing Configuration Confirmation Dialog Box

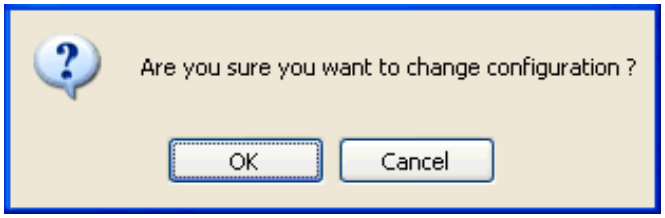

Figure 3-28 Configuration Confirmation Dialog Box

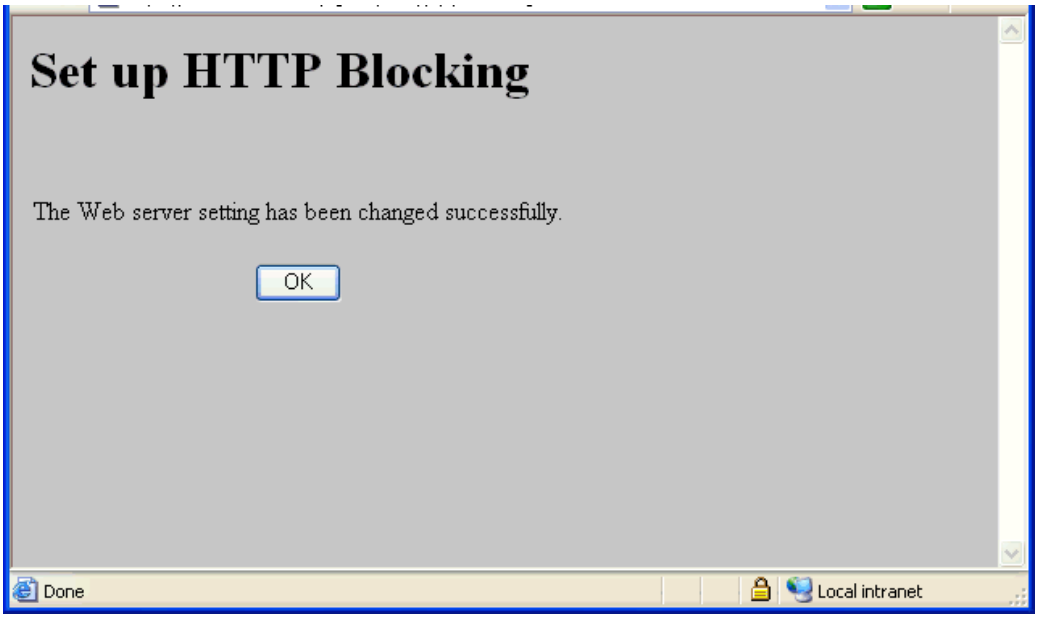

Figure 3-29 Set Up HTTP Blocking Completion Dialog Box

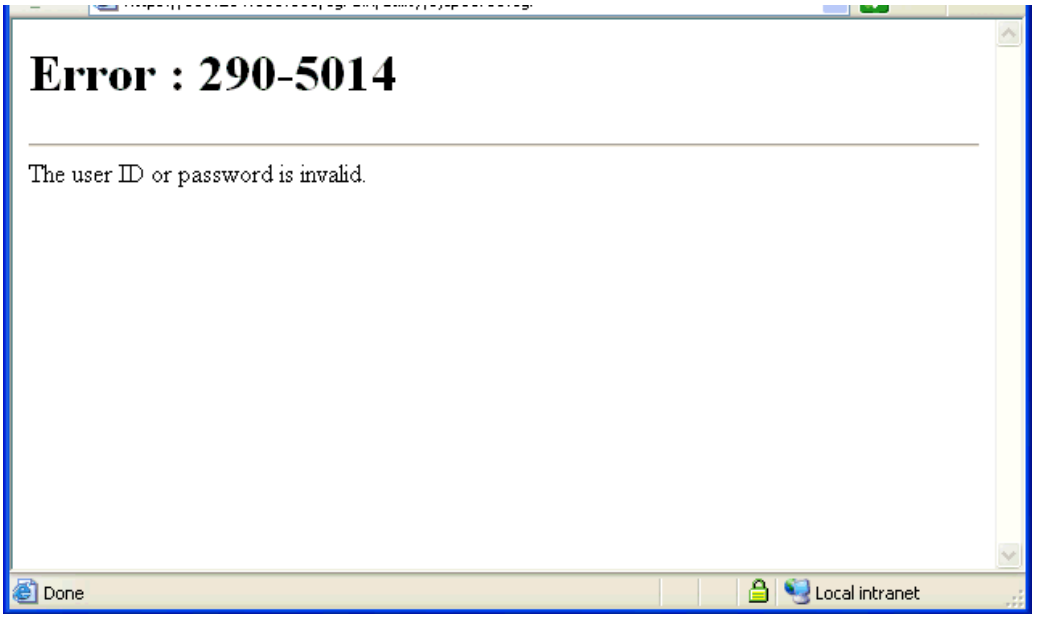

Figure 3-30 Set Up HTTP Blocking Error Message Dialog Box

Releasing HTTP Communication Blocking

To release HTTP communication blocking:

1. Log off all Storage Navigator computers connected to the web server (SVP).
2. Start both Storage Navigator and your web browser.

3. If you are using TagmaStore USP or NSC, specify the following URL to open the **Release HTTP Blocking** logon dialog box:

   https://*xxx.xxx.xxx.xxx*/cgi-bin/utility/sjcp80rel.cgi

   where *xxx.xxx.xxx.xxx* is the IP address or host name of the SVP.

   If you are using USP V/VM:

   a. Specify the following URL to open the **Tool Panel** dialog box:

      https://*xxx.xxx.xxx.xxx*/cgi-bin/utility/toolpanel.cgi

      where *xxx.xxx.xxx.xxx* is the IP address or host name of the SVP.

   b. On the Tool Panel dialog box (Figure 3-31), click **Release HTTP Blocking**.

4. Type the User ID and Password for the root storage administrator, and then click **Logon** (Figure 3-32).
5. In the **Release HTTP Blocking** dialog box (Figure 3-33), click **OK**.
6. In the configuration confirmation dialog box (Figure 3-28), click **OK**.
7. When the configuration change is complete, the web server reboots and the Release HTTP Blocking Complete dialog box opens (Figure 3-34). Click **OK**; you will return to the Logon dialog box.

If an error occurs during the operation, an error message will appear (Figure 3-30). Solve the problem and restart from the logging on to **Release HTTP Blocking.**

After releasing HTTP communication blocking, you must change the configuration of the Storage Device List. For details, see Editing the Storage Device List.

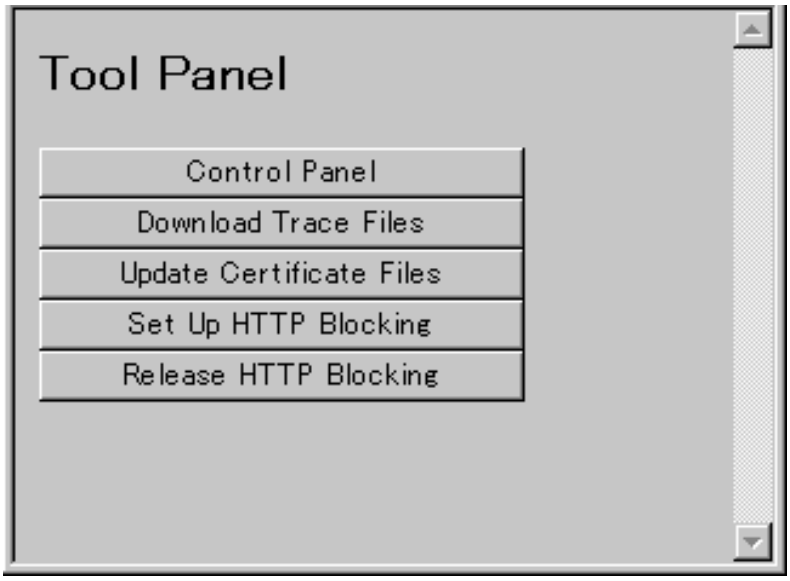

Figure 3-31 Tool Panel Dialog box

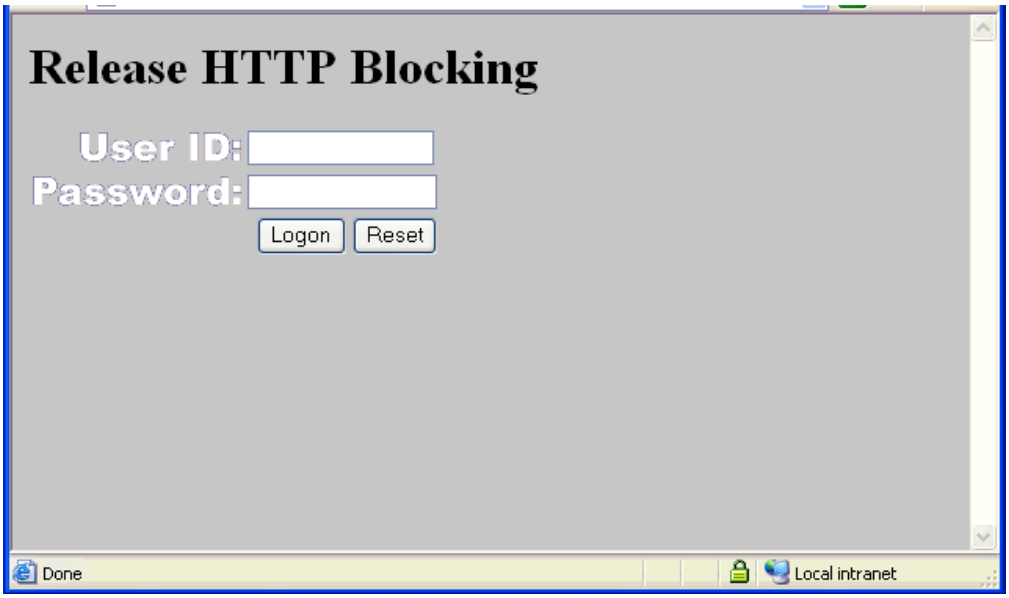

Figure 3-32 Release HTTP Blocking Logon Dialog Box

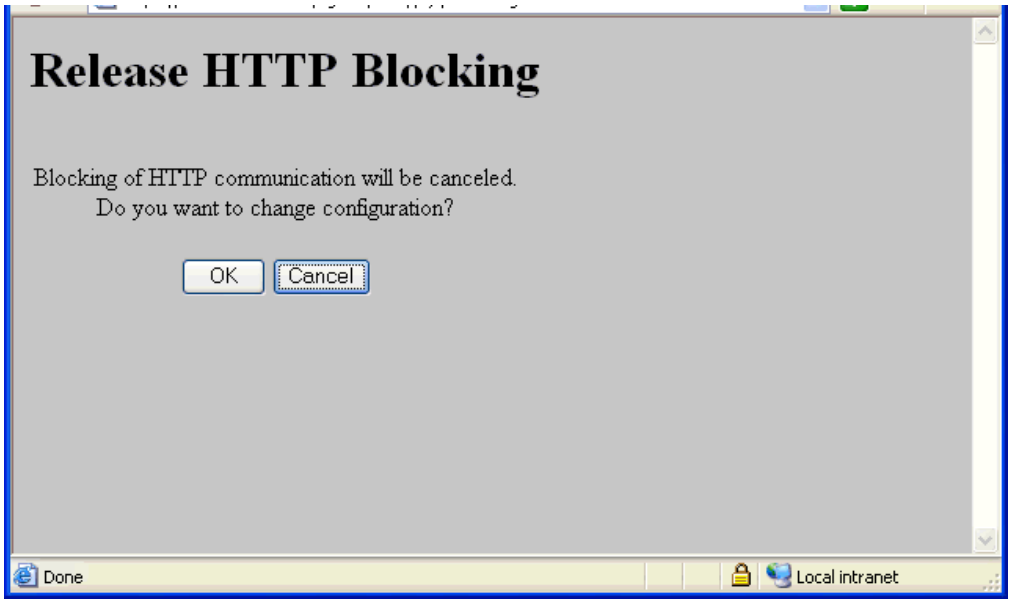

Figure 3-33 Changing Configuration of Release HTTP Blocking Dialog Box

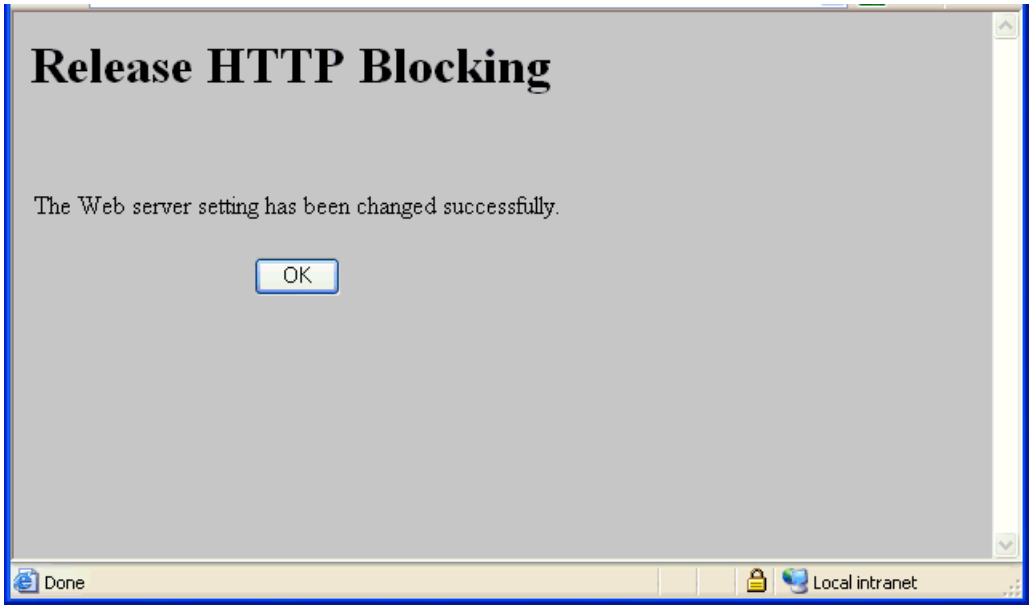

Figure 3-34 Release HTTP Blocking Completion Dialog Box

Editing the Storage Device List

After setting up or releasing HTTP communication blocking, you must change the configuration of the Storage Device List. By default, the Storage Device List configuration enables Storage Navigator to use HTTP communication. For details on how to set up the Storage Device List, please refer to the *Storage Navigator User's Guide*.

- On the **Storage Entry** dialog box (Figure 3-35) or the **Change Storage Entry** dialog box (Figure 3-36), check **SVP which has blocked out HTTP** and click **Submit**.
- After releasing HTTP communication blocking:

  On the **Change Storage Entry** dialog box, clear the **SVP which has blocked out HTTP** check box in **HTTP Block**, and then click **Submit**.
- When you use HTTP communication:

  On the **Storage Entry** dialog box or the **Change Storage Entry** dialog box, clear the **SVP which has blocked out HTTP** check box in **HTTP Block**, and then click **Submit**.

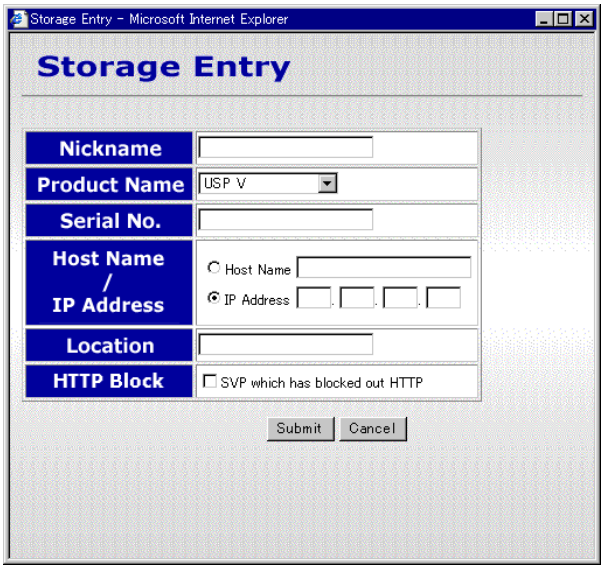

Figure 3-35 Storage Entry Dialog Box

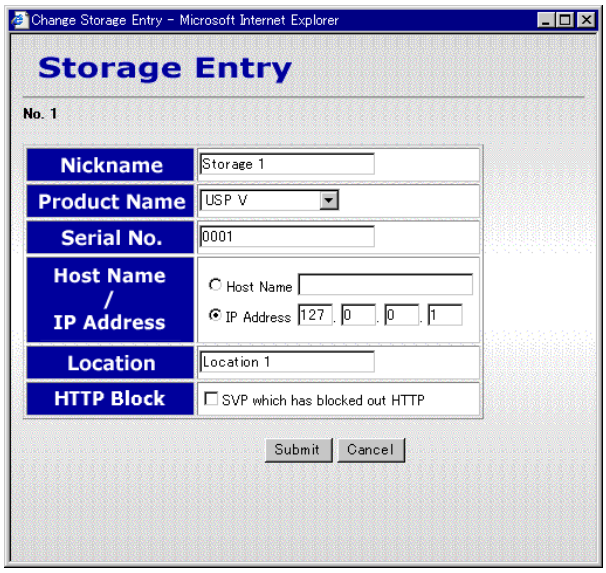

Figure 3-36 Change Storage Entry Dialog Box

4

Troubleshooting

This chapter provides general troubleshooting information:

- ☐ General Troubleshooting
- ☐ Calling the Hitachi Data Systems Support Center

General Troubleshooting

For troubleshooting information on the Hitachi storage system, refer to the *User and Reference Guide* for the storage system.

For troubleshooting information on Storage Navigator, see the *Storage Navigator User's Guide* for the storage system.

If you need technical assistance, call the Hitachi Data Systems Support Center (see Calling the Hitachi Data Systems Support Center).

Calling the Hitachi Data Systems Support Center

If you need to call the Hitachi Data Systems Support Center, please provide as much information about the problem as possible, including:

- The circumstances surrounding the error or failure.
- The content of any error message(s) displayed on the host system(s).
- The content of any error message(s) displayed on Storage Navigator.
- The Storage Navigator configuration information (use the FD Dump Tool).
- The service information messages (SIMs), including reference codes and severity levels, displayed by Storage Navigator.

The Hitachi Data Systems customer support staff is available 24 hours/day, seven days a week. If you need technical support, please call:

- United States: (800) 446-0744
- Outside the United States: (858) 547-4526

Acronyms and Abbreviations

CA	Certificate Authority
CD	compact disk
CSR	Certificate Signing Request
FD	floppy disk
FTP	file transfer protocol
GB	gigabyte (see Convention for Storage Capacity Values)
GUI	graphical user interface
HTTP	hypertext transfer protocol
HTTPS	hypertext transfer protocol – secure
IP	internet protocol
KB	kilobyte (see Convention for Storage Capacity Values)
LAN	local-area network
MB	megabyte (see Convention for Storage Capacity Values)
NSC	Hitachi TagmaStore Network Storage Controller
PB	petabyte (see Convention for Storage Capacity Values)
SIM	service information message
SSL	secure sockets layer
SVP	service processor
TB	terabyte (see Convention for Storage Capacity Values)
URL	universal resource locator
USP	Hitachi TagmaStore Universal Storage Platform
USP V	Hitachi Universal Storage Platform V
USP VM	Hitachi Universal Storage Platform VM
VOL	volume
WWN	world wide name

Index

Hitachi Data Systems

Corporate Headquarters
750 Central Expressway
Santa Clara, California 95050-2627
U.S.A.
Phone: 1 408 970 1000
www.hds.com
info@hds.com

Asia Pacific and Americas
750 Central Expressway
Santa Clara, California 95050-2627
U.S.A.
Phone: 1 408 970 1000
info@hds.com

Europe Headquarters
Sefton Park
Stoke Poges
Buckinghamshire SL2 4HD
United Kingdom
Phone: + 44 (0)1753 618000
info.eu@hds.com

Hitachi Data Systems

MK-96RD631-04