



LIVE BACKUP AND SSL

Configuring secure connections with Live Backup using HTTPS



Sept 2010



CONTENTS

INTRODUCTION	3
OBTAIN A CERTIFICATE FOR SSL COMMUNICATION	3
OBTAIN A CERTIFICATE UNDER WINDOWS SERVER 2003	4
GENERATE A CERTIFICATE REQUEST	4
SUBMIT THE CERTIFICATE REQUEST	9
ISSUE THE CERTIFICATE OR OBTAIN IT FROM ONE OF EXISTING AUTHORITIES.	12
CONFIGURE SSL IN LIVE BACKUP'S VIRTUAL WEB SITES IN IIS	12
OBTAIN A CERTIFICATE UNDER WINDOWS SERVER 2008	13
CREATE THE CERTIFICATE SIGNING REQUEST	13
INSTALL THE CERTIFICATE	17
BIND THE CERTIFICATE TO A WEBSITE	19
CONFIGURE CLIENTS TO TRUST THE SERVER CERTIFICATE	21
ADD THE CERTIFICATES SNAP-IN FOR CURRENT USER AND LOCAL COMPUTER	21
ADD THE CERTIFICATES SNAP-IN FOR THE LOCAL SYSTEM ACCOUNT	23
CONFIGURE THE CURRENT USER TO TRUST THE CERTIFICATE	23
CONFIGURE THE LOCAL COMPUTER TO TRUST THE CERTIFICATE	25
CONFIGURE LIVE BACKUP CLIENT TO COMMUNICATE OVER HTTPS	26

INTRODUCTION

Live Backup can support secure communications between the server and client components over HTTPS. This document provides instructions for configuring Live Backup to use HTTPS for data transport.

This document assumes a working knowledge of certificates, SSL, and HTTPS. Although it provides basic instructions for adding and configuring certificates, it is not intended to be a comprehensive description of the setup process or use of Microsoft certificates for security. For more detailed information, go to the Microsoft Web site, or contact Microsoft support.

Before continuing, note that the transport performance between the Live Backup client and server decreases when using HTTPS, because HTTPS leads to higher CPU usage on the client and server. Before continuing with this procedure, carefully consider the impact of this performance degradation on your environment.

The basic setup process includes the following steps:

1. Obtain a certificate for SSL communication
2. Configure SSL in Live Backup's virtual Web sites in IIS using a certificate
3. Configure clients to trust the server certificate (optional)
4. Configure Live Backup Client to accept HTTPS communications

The remainder of this document describes the individual steps required to complete the process above.

NOTE Mac Client Updates--both notifications and download--must be delivered over HTTP, not HTTPS. To learn how to configure ports, see "Changing ports used for server/client communication" in Appendix A of the *Live Backup Installation and Setup Guide*

OBTAIN A CERTIFICATE FOR SSL COMMUNICATION

To configure Live Backup to use SSL, you must first install a certificate on the Live Backup Server. Atempo recommends that you use a certificate that is signed by one of the pre-installed Authorities in Microsoft Windows, such as VeriSign. For more information on using an existing certificate and any cost associated with it, contact the selected authorities (such as VeriSign).

How you obtain a certificate depends on which version of Microsoft Windows you are using: Windows Server 2003 or Windows Server 2008.

OBTAIN A CERTIFICATE UNDER WINDOWS SERVER 2003

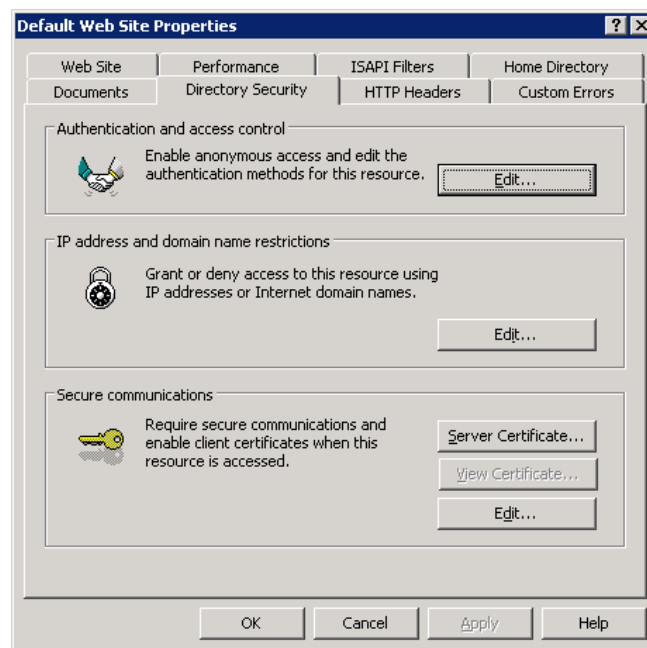
This section describes how to obtain, install and configure a certificate for SSL communication under Windows Server 2003. The steps in this process include the following:

1. Generate a Certificate Request
2. Submit the Certificate Request
3. Issue the Certificate or obtain it from one of existing Authorities.

GENERATE A CERTIFICATE REQUEST

To begin, you must create a new certificate request, which can then be sent to a Certification Authority for processing.

1. On the Live Backup Server run IIS: Click **Start**, point to **Programs**, point to **Administrative tools**, and then click **Internet Services Manager**.
2. Expand the **Live Backup Server name**, and then expand **Web sites**.
3. Right-click the **Default Web site**, and then click **Properties**.
4. Click the **Directory Security** tab.



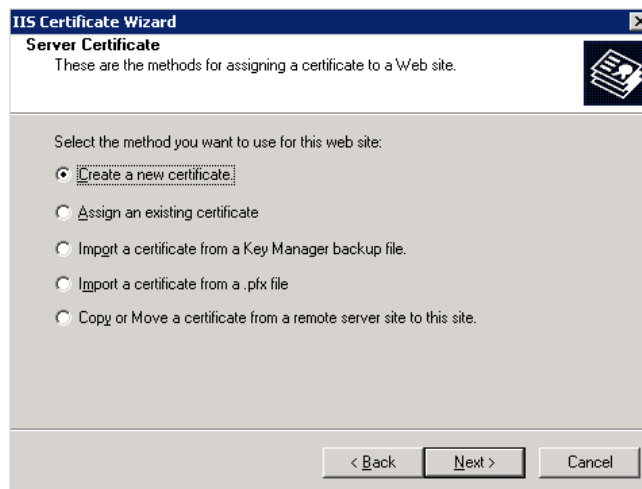
5. On the Directory Security page, under the Secure Communications group box, click the **Server Certificate** button.

The Web Server Certificate Wizard appears.

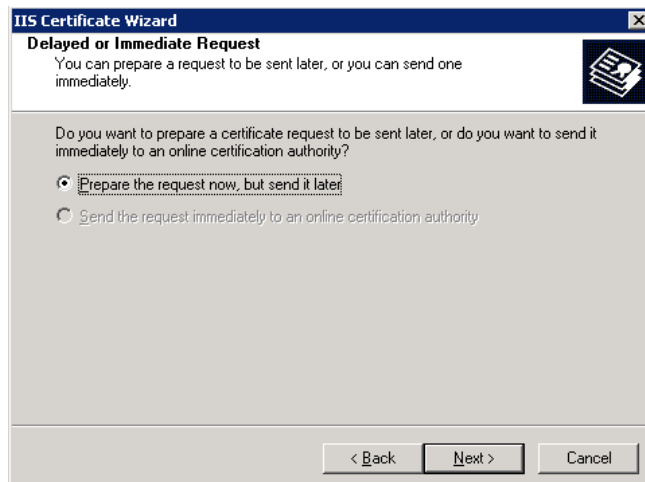


6. Click **Next**.

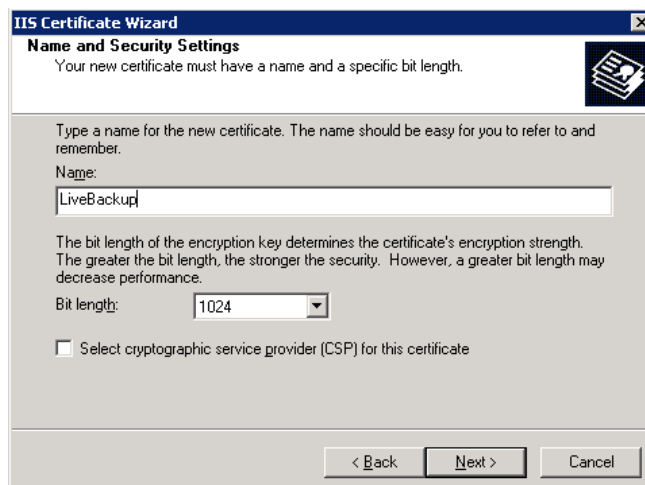
7. On the Server Certificate page, click **Create a New Certificate**, and then click **Next**.



- On the Delayed or Immediate Request page, click **Prepare the request now, but send it later**, and then click **Next**.

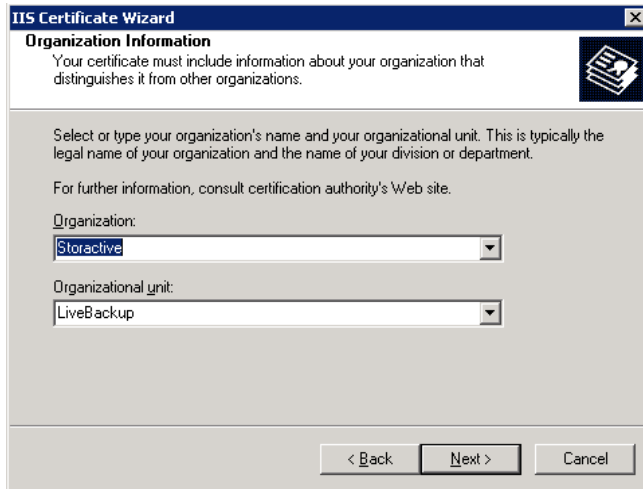


- On the Name and Security Settings page, type a descriptive name for the certificate in the **Name** box; type a bit length for the key in the **Bit length** box, and then click **Next**.



By default, the wizard uses the name of the current Web site as a default name. It is not used in the certificate but acts as a friendly name to help administrators. Since Live Backup uses the default Web site, you may want use the name "Live Backup" in the Name field.

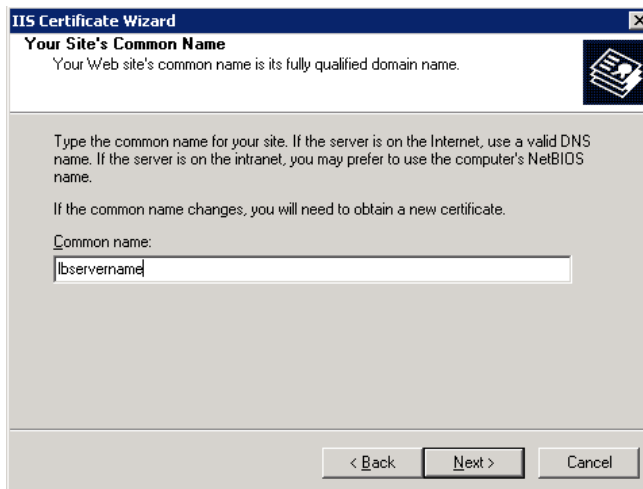
10. On the Organization Information page, type an organization name in the **Organization** box and type an organizational unit in the **Organizational unit** box, and then click **Next**.



The screenshot shows the 'IIS Certificate Wizard' window with the 'Organization Information' tab selected. The window title is 'IIS Certificate Wizard' and the subtitle is 'Organization Information'. Below the subtitle, there is a note: 'Your certificate must include information about your organization that distinguishes it from other organizations.' The main area contains instructions: 'Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department. For further information, consult certification authority's Web site.' There are two dropdown menus: 'Organization' with 'Storactive' selected and 'Organizational unit' with 'LiveBackup' selected. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

This information will be placed in the certificate request, so make sure it is accurate. The CA will verify this information and will place it in the certificate. A user browsing your Web site will want to see this information in order to decide if they should accept the certificate.

11. On the Your Site's Common Name page, in the **Common name** box, type a common name for your site, and then click **Next**.



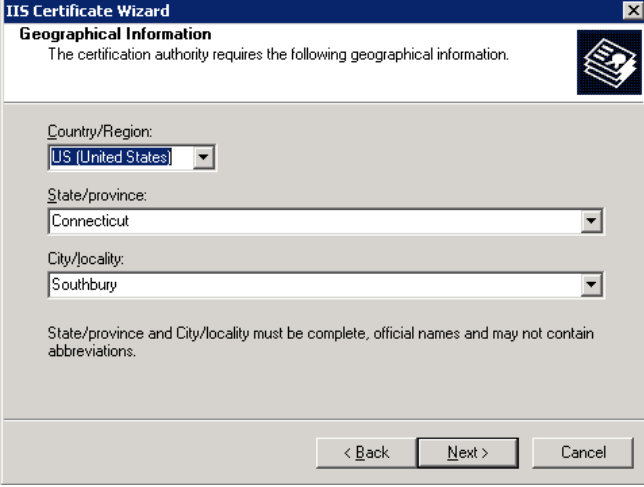
The screenshot shows the 'IIS Certificate Wizard' window with the 'Your Site's Common Name' tab selected. The window title is 'IIS Certificate Wizard' and the subtitle is 'Your Site's Common Name'. Below the subtitle, there is a note: 'Your Web site's common name is its fully qualified domain name.' The main area contains instructions: 'Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name. If the common name changes, you will need to obtain a new certificate.' There is a text input field labeled 'Common name:' with 'lbservername' entered. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

The common name is one of the most significant pieces of information that ends up in the certificate. It is the DNS name of the Web site (that is, the name that users type in when browsing your site).

For Live Backup, use the name of the Live Backup Server computer. For example, if the name of your Live Backup Server is **lbserver**, then type **lbserver** into the **Common name** box. If you do not use the correct name then SSL will not work.

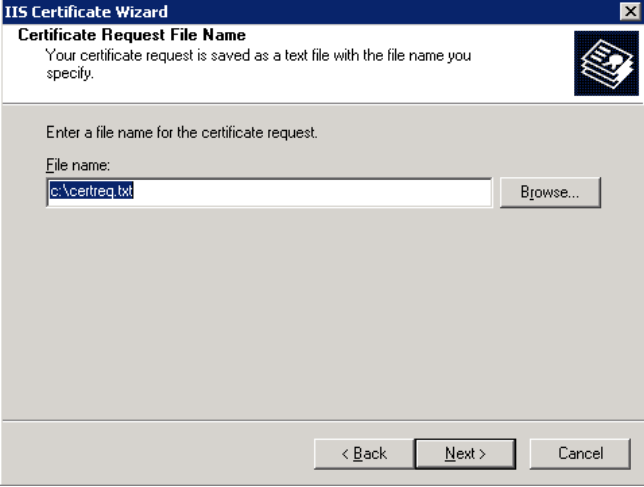
Note that if the server has several DNS names, use only one that Live Backup clients use to access the server. If you don't, then the connection via https cannot be established because the URL in the certificate will not match the real URL.

12. On the Geographical Information page, enter the appropriate information in the **Country/Region**, **State/province**, and **City/locality** boxes, and then click **Next**.



The screenshot shows the 'IIS Certificate Wizard' window, specifically the 'Geographical Information' step. The title bar reads 'IIS Certificate Wizard' and the subtitle is 'Geographical Information'. Below the subtitle, it says 'The certification authority requires the following geographical information.' There are three dropdown menus: 'Country/Region' with 'US (United States)' selected, 'State/province' with 'Connecticut' selected, and 'City/locality' with 'Southbury' selected. A note at the bottom states: 'State/province and City/locality must be complete, official names and may not contain abbreviations.' At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

13. On the Certificate Request File Name page, type a file name for the certificate request (by default, certreq.txt). Note the location of the file, as you will need it later. Click **Next**.



The screenshot shows the 'IIS Certificate Wizard' window, specifically the 'Certificate Request File Name' step. The title bar reads 'IIS Certificate Wizard' and the subtitle is 'Certificate Request File Name'. Below the subtitle, it says 'Your certificate request is saved as a text file with the file name you specify.' There is a text input field labeled 'File name:' containing 'c:\certreq.txt' and a 'Browse...' button to its right. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

14. Check the information in the Summary page, and then click **Finish** to complete the request.

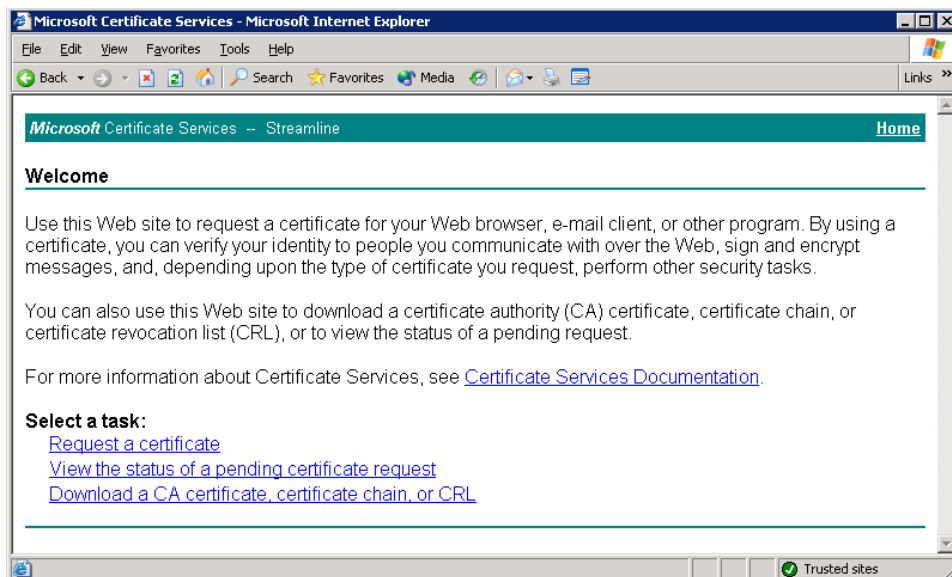
SUBMIT THE CERTIFICATE REQUEST

Now that you have generated the certificate request, you must submit it for authorization.

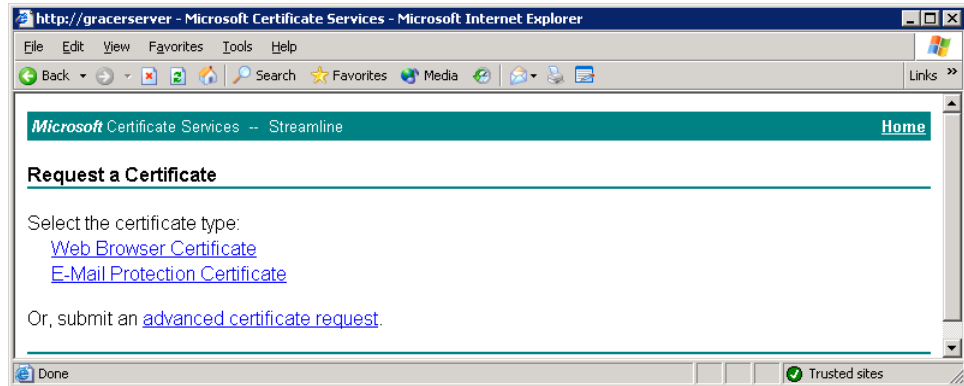
It is recommended that you use one of pre-installed Authorities such as VeriSign. Send the request that is generated on the previous step to them. You can also use your own Authority system, for example, Microsoft Certificate Services. Note that if you use your own authority system you have to configure the root certificate for this Authority as trusted on all client computes (see 3 “Configure clients to trust the server certificate” for detail)

Use a text editor to open the Certificate Request generated in the previous procedure and copy the text the clipboard.

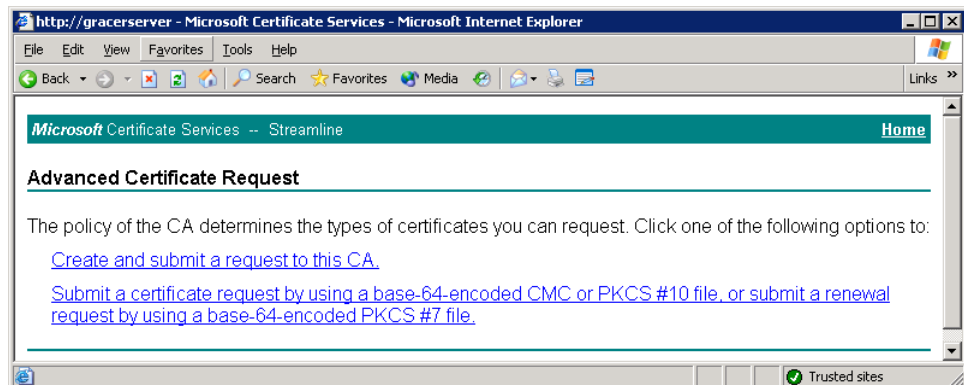
1. Run Microsoft Certificate Services: Open Internet Explorer and go to <http://hostname/CertSrv>, where *hostname* is the name of the Live Backup Server computer.



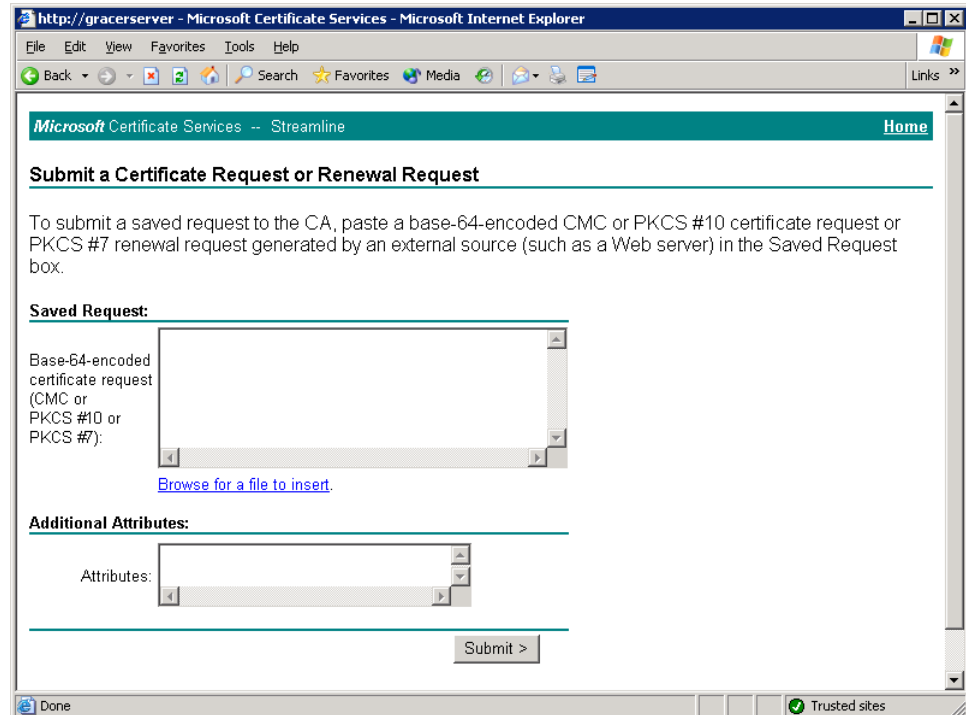
2. Click **Request a certificate**.



3. Click **advanced certificate request**.



4. Click **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**.



5. In the **Saved Request** box, paste the contents of the certificate file that you copied to the clipboard in step 1, and then click **Submit**.
6. Close Internet Explorer.

ISSUE THE CERTIFICATE OR OBTAIN IT FROM ONE OF EXISTING AUTHORITIES.

You can now issue the certificate. If you just received it from one of Authorities, skip these steps and start with Configure SSL in Live Backup's virtual Web sites in IIS, as described below

To complete this procedure, you need the Certification Authority tool in Windows. A shortcut should be located in the Administrative Tools program group. If you do not see it here, you will need to install it from your Windows CD.

TO INSTALL THE CERTIFICATION AUTHORITY TOOL:

1. On the Live Backup Server, click **Start**, point to **Control Panel**, and then click **Add/Remove Programs**.
2. In the Add/Remove Programs window, click **Add/Remove Windows Components**.
3. In the Windows Components Wizard, select **Certificate Services**, and then complete the wizard to install. You will need your Windows Server CD.

TO ISSUE THE CERTIFICATE:

1. On Live Backup Server, run the Certification Authority tool: Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Certification Authority**.
2. Expand your certificate authority, and then click **Pending Requests**.
3. Right-click the certificate request you just submitted, and then click **Issue**.
4. In the console tree, click **Issued Certificates**. The certificate should appear here.
5. Double-click the certificate.
6. In Certificate Properties, click the **Details** tab.
7. On the Details page, click **Copy to File**, and save the certificate as a Base-64 encoded X.509 certificate.
8. Close Certificate Properties, and then close the Certification Authority Tool.

CONFIGURE SSL IN LIVE BACKUP'S VIRTUAL WEB SITES IN IIS

To configure Live Backup to communicate using SSL, you must install the certificate on the Live Backup Web server. You can do this under the Default Web site in IIS. Once you install the certificate, Live Backup's virtual Web sites (LBClient and WLB) will also use these settings.

1. Run IIS.
2. Expand the *servername*, and then expand **Web sites**.
3. Right-click **Default Web site**, and then click **Properties**.
4. On the Properties dialog box, click the **Directory Security** tab.

5. On the Directory Security page, click the **Server Certificate** button.
6. In the Welcome page of the Web Server Certificate Wizard, click **Next**.
7. Click **Process the pending request and install the certificate**, and then click **Next**.
8. Locate and select the .cer file you exported in the previous procedure.
9. Leave SSL port at 443, and then complete the wizard.
10. Exit IIS.

Note To ensure that Live Backup can continue to service both HTTP and HTTPS requests, you need to make sure that the **Require secure channel (SSL)** option is *cleared* under Directory Security\Secure Communications (Edit) for both the LBClient and the WLB Web sites. If this option is selected, then you must configure all of your Live Backup Clients to use HTTPS.

OBTAIN A CERTIFICATE UNDER WINDOWS SERVER 2008

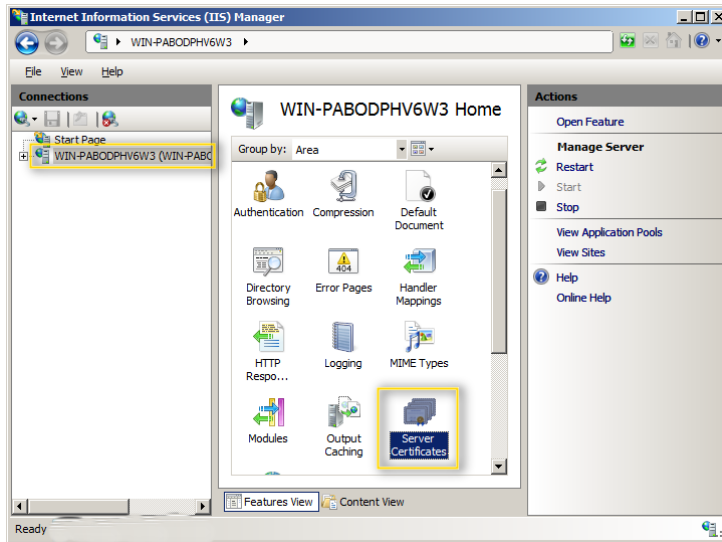
The following section describes how to

- Create the certificate request
- Install under IIS 7 on Windows Server 2008

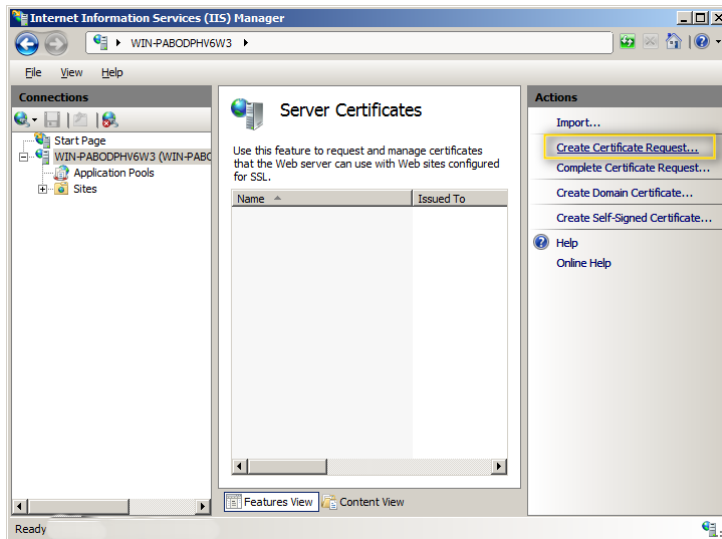
CREATE THE CERTIFICATE SIGNING REQUEST

The first step in ordering an SSL certificate is generating a [Certificate Signing Request](#).

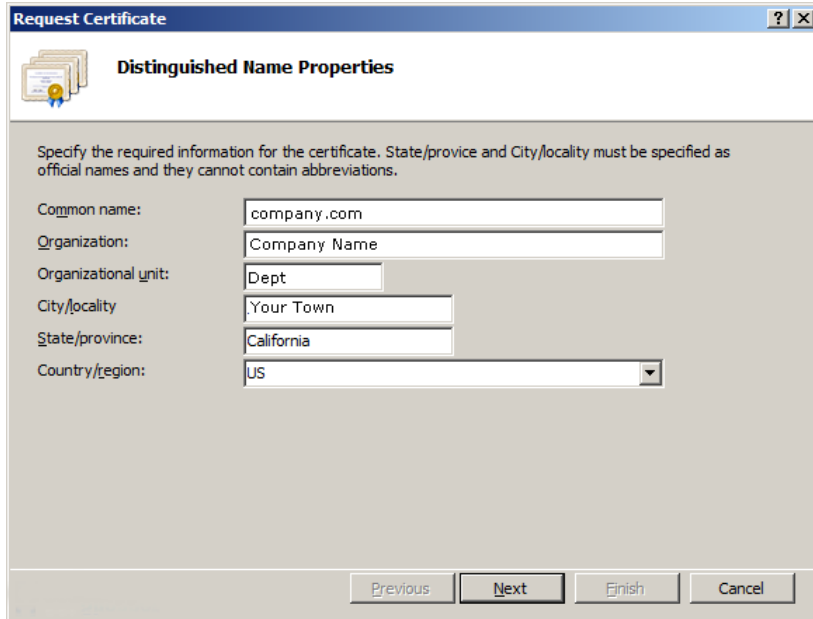
1. Click **Start**, go to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In the **Connections** column, click the name of the server. Then in the center pane, double-click **Server Certificates**.



3. In the Actions column on the right, click **Create Certificate Request...**



The Request Certificate Wizard appears.

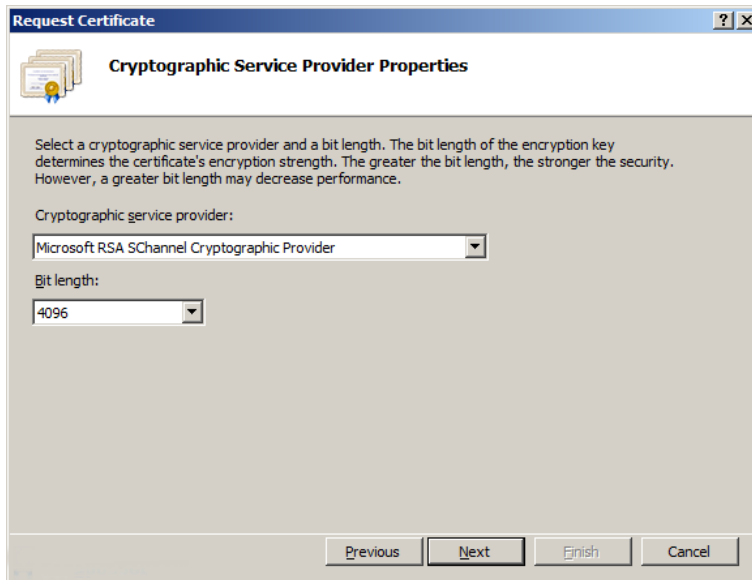


4. On the Distinguished Name Properties page, enter domain and company information.

NAME	EXPLANATION	EXAMPLES
Common Name	The fully qualified domain name (FQDN) of your server. This must match exactly what you type in your web browser.	*.company.com
Organization	The legal name of your organization. This should not be abbreviated and should include suffixes such as Inc, Corp, or LLC.	Company Inc.
Organizational Unit	The division of your organization handling the certificate.	Information Technology
City/Locality	The city where your organization is located.	New York
State/province	The state/region where your organization is located. This shouldn't be abbreviated.	California
Country/Region	The two-letter ISO code for the country where your organization is location.	US

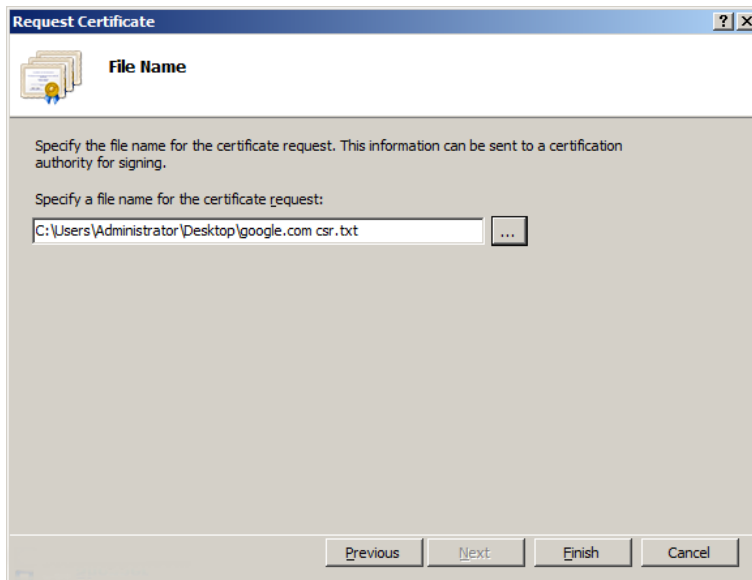
Click **Next**.

The Cryptographic Service Provider Properties page appears.



5. Leave the default **Cryptographic Service Provider**. Increase the Bit length if desired. Higher is more secure but slower. Click **Next**.

The File Name page appears.



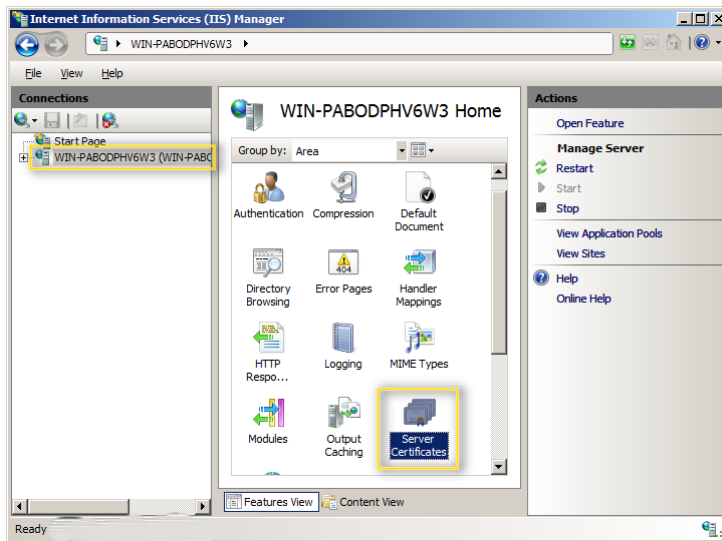
6. Beside **Specify a file name for the certificate request**, click the ellipses button . . . , and then type a location and filename where you want to save the CSR file. Click **Finish**.

Once you have generated a CSR you can use it to order the certificate from a [certificate authority](#). Once you complete the ordering process, during which you will paste the contents of the CSR text file, and your order is validated, you will receive the SSL certificate file.

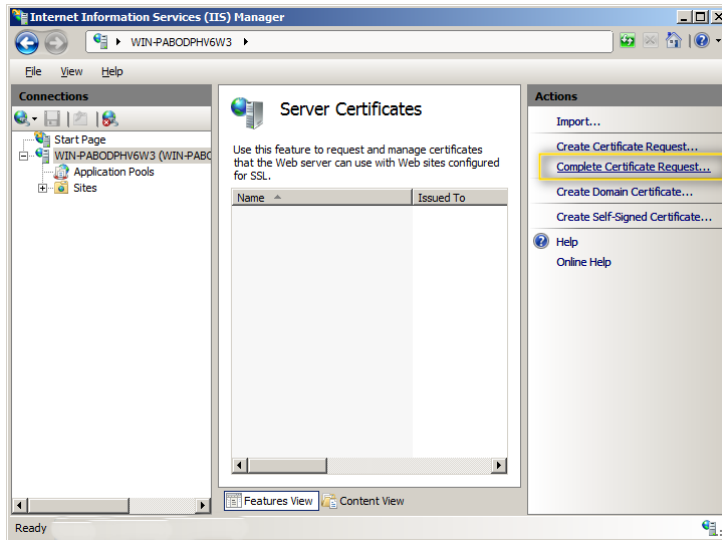
INSTALL THE CERTIFICATE

To install your newly acquired SSL certificate in IIS 7, first copy the file somewhere on the server and then follow these instructions:

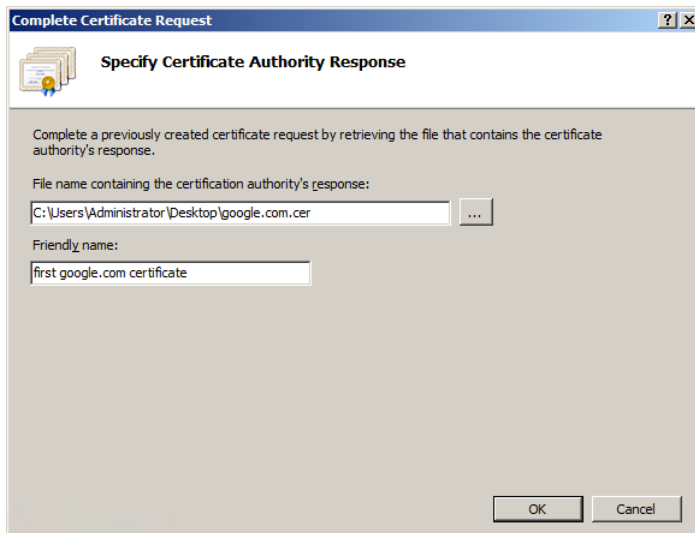
1. Click the **Start** menu, go to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In the **Connections** column, click the name of the server. Double-click **Server Certificates**.



3. In the **Actions** column on the right, click **Complete Certificate Request...**

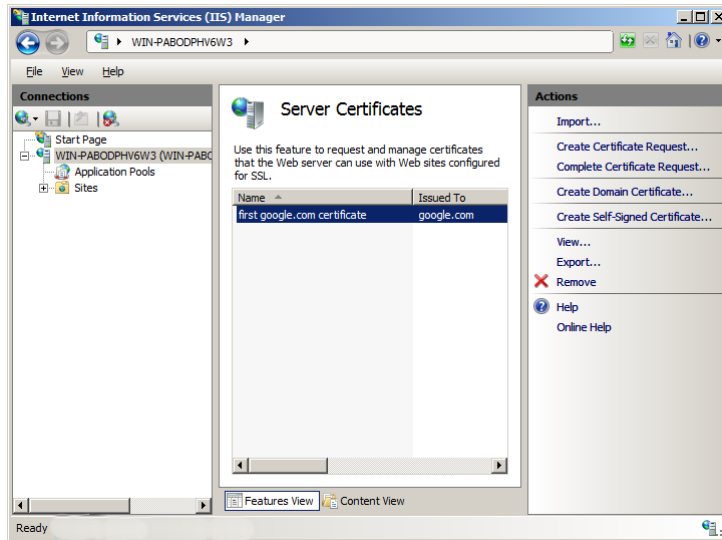


The Complete Certificate Authority Response Wizard appears.



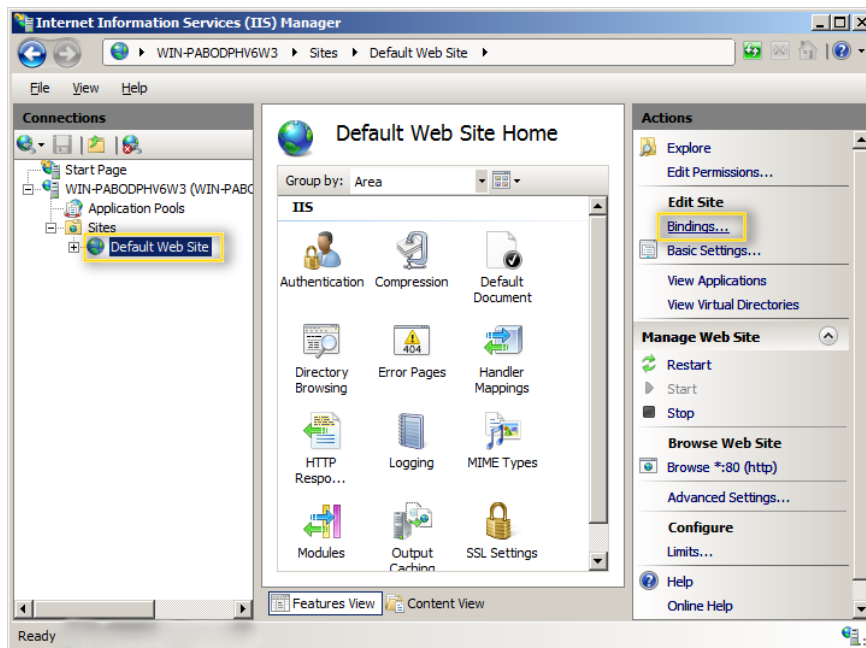
4. On the Specify Certificate Authority Response page, click the **ellipses** button . . . , and then select the server certificate that you received from the certificate authority. If the certificate doesn't have a .cer file extension, view all types. You may use any name you want, but make sure to keep the cer extension. Click **OK**.

If successful, you will see your newly installed certificate in the list. If you receive an error stating that the request or private key cannot be found, make sure you are using the correct certificate and that you are installing it to the same server on which you generated the CSR. If you are sure of those two things, you may just need to create a new Certificate Request and reissue/replace the certificate. If you have any problems, contact your certificate authority.

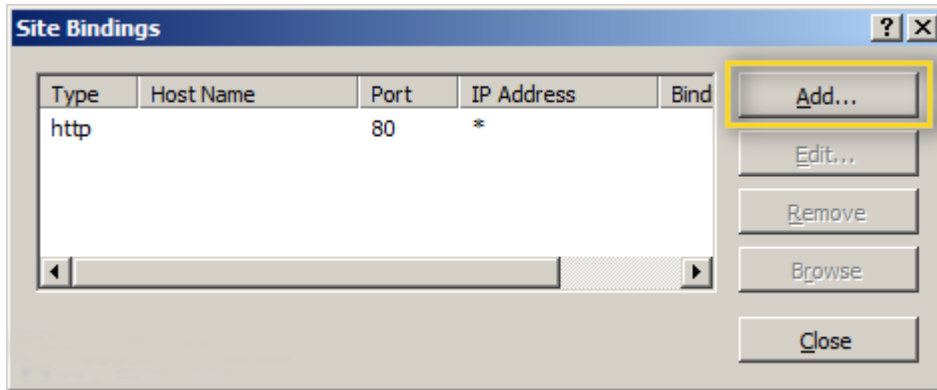


BIND THE CERTIFICATE TO A WEBSITE

1. In the **Connections** column, expand the **Sites** folder, and then click the web site to which you want to bind the certificate.
2. In the **Actions** column on the right, under **Edit Site**, click **Bindings**.



The Site Bindings dialog box appears.

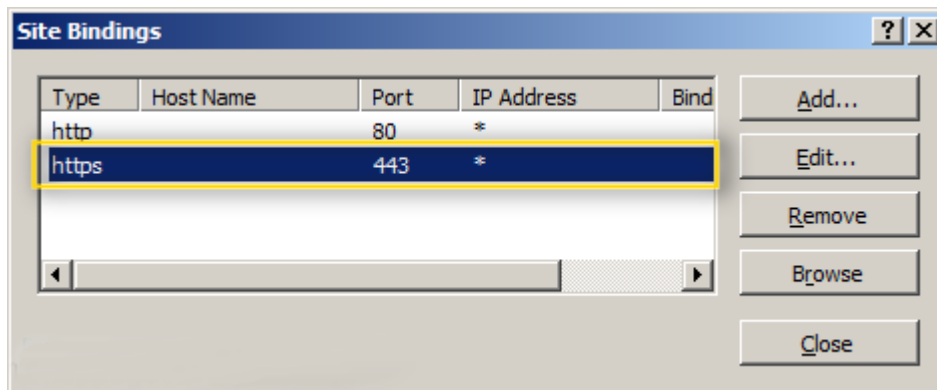


3. Click **Add**.

The Add Site Binding dialog box appears.



4. From the **Type** list, select **https**. Then From the **SSL certificate** list, select the SSL certificate that you just installed. Click **OK**.
5. You will now see the binding for port 443 listed. Click **Close**.



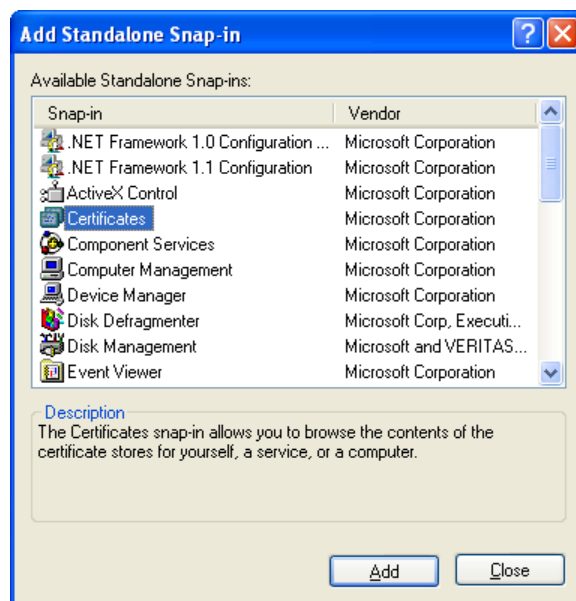
CONFIGURE CLIENTS TO TRUST THE SERVER CERTIFICATE

If the certificate used on the server is signed by one of preinstalled trusted Authorities, you don't need to complete these steps. If not, you must configure the Live Backup Client to trust the server certificate. When Live Backup Client attempts to connect to Live Backup Server, the connection will be authenticated using the certificate. If the certificate is not trusted, then the connection will fail.

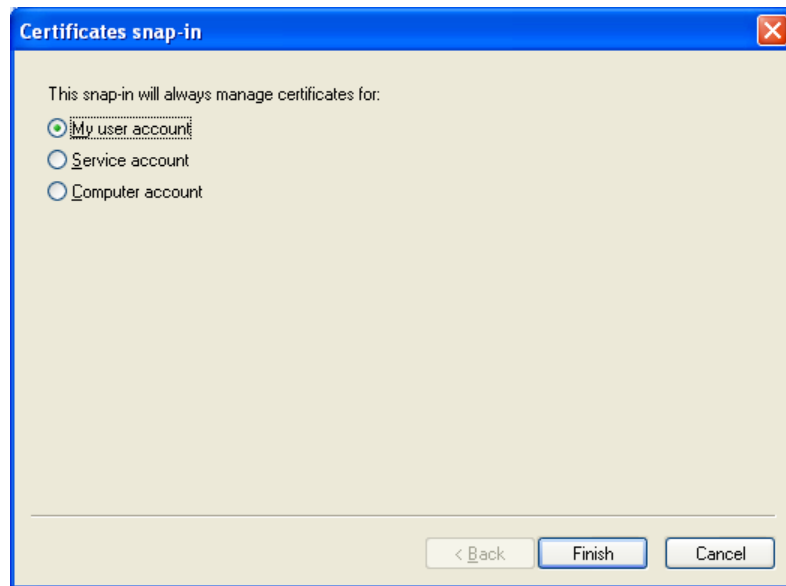
To configure the client to trust the certificate, you must add the certificate to the Trusted Root Certification Authority for the Current User, Local System Account, and all users that can use Live Backup Client and the Local Computer in the Certificates snap-in on the client computer.

ADD THE CERTIFICATES SNAP-IN FOR CURRENT USER AND LOCAL COMPUTER

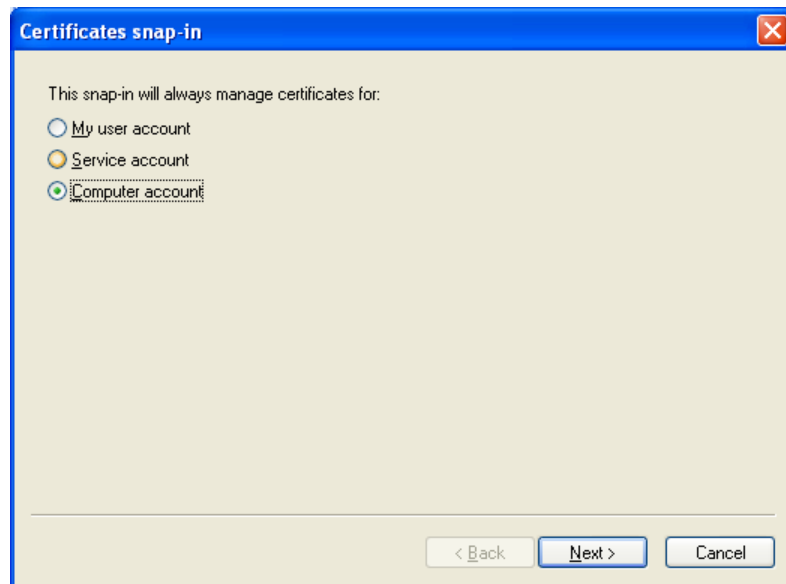
1. On the Live Backup Client, run Microsoft Management Console: Click **Start**, and then click **Run**. Type **mmc**, and then click **OK**.
2. From the **File** menu, click **Add/Remove Snap-in**.
3. In the Add/Remove Snap-in dialog box, click **Add**.
4. In the Add Standalone Snap-in dialog box, click **Certificates**, and then click **Add**.



5. In the Certificates Snap-in Wizard, click **My user account**, and then click **Finish**.



6. Repeat steps 4 and 5, but select **Computer account** instead of My user account.



7. In the Add Standalone Snap-ins dialog box, click **Close**.
8. In the Add/Remove Snap-in dialog box, click **OK**.
9. Do not close the Certificates snap-in.

ADD THE CERTIFICATES SNAP-IN FOR THE LOCAL SYSTEM ACCOUNT

1. If you don't have it already, download **cmdasuser.exe** from <ftp://ftp.atempo.com/private/LiveBackup/cmdasuser.exe>.
2. Run cmdasuser.exe: Click **Start**, and then click then **Run**. In the Run dialog box, type the path where you downloaded the tool, followed by **CMDASUSER.EXE localsystem**

The command prompt window appears running under the local system account.

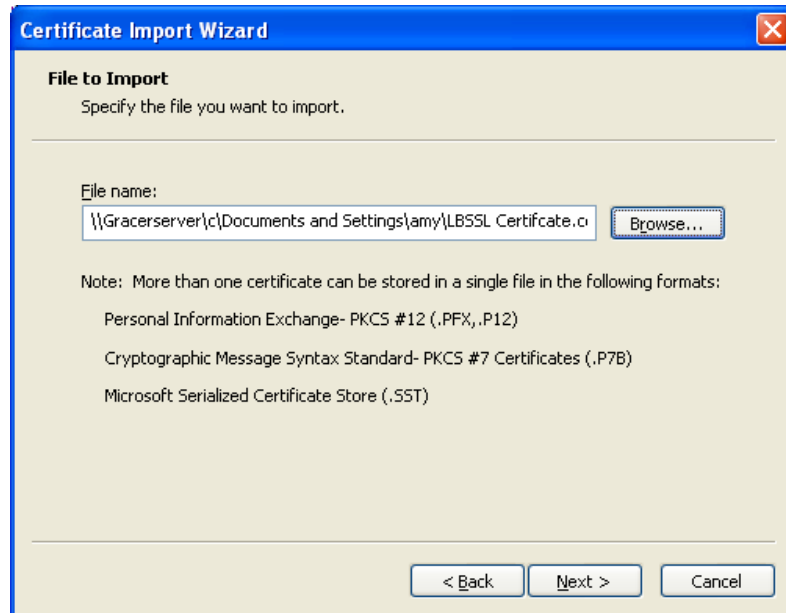
3. In the window that appears, type **mmc**. MMC console will start under the Local System account.
4. Repeat the procedure, Add the Certificates snap-in for Current User and Local Computer on page 21.

CONFIGURE THE CURRENT USER TO TRUST THE CERTIFICATE

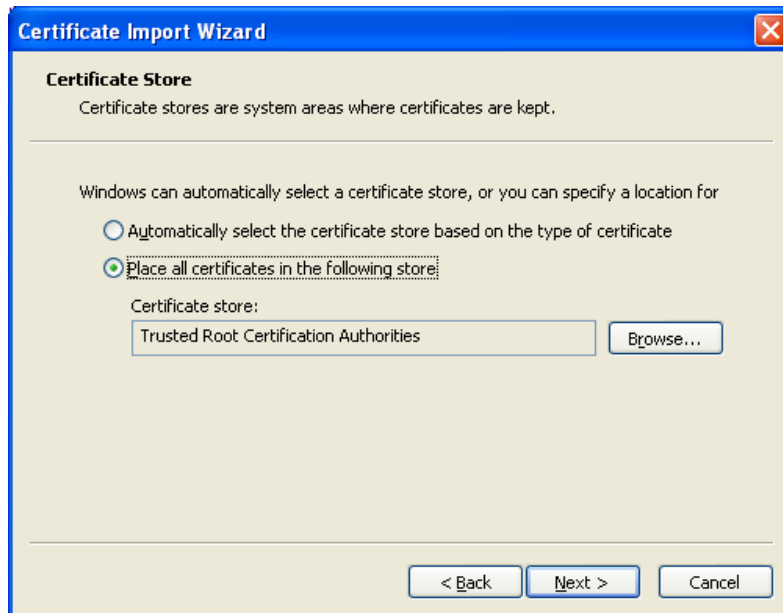
1. Expand **Certificates—Current User**, and then click **Trusted Root Certification Authorities**.
2. Right-click **Certificates**, point to **All Tasks**, and then click **Import**.



3. On the Welcome page of the Certificate Import Wizard, click **Next**.



4. On the File to Import page, click **Browse**, and select the location of the *.cer file you saved earlier. Click **Next**.



5. On the Certificate Store page, select **Place all Certificates in the following store**, and then choose **Trusted Root Certification Authorities**. Click **Next**.
6. Click **Finish**.

CONFIGURE THE LOCAL COMPUTER TO TRUST THE CERTIFICATE

Repeat the same steps for the Local Computer Certificates...

1. Expand **Certificates—Local Computer**, and then click **Trusted Root Certification Authorities**.
2. Right-click **Certificates**, point to **All Tasks**, and then click **Import**.
3. On the Welcome page of the Certificate Import Wizard, click **Next**.
4. On the File to Import page, click **Browse**, and select the location of the *.cer file you saved earlier. Click **Next**.
5. On the Certificate Store page, select **Place all Certificates in the following store**, and then choose **Trusted Root Certification Authorities**. Click **Next**.
7. Click **Finish**.

CONFIGURE LIVE BACKUP CLIENT TO COMMUNICATE OVER HTTPS

The final step in this process is to configure the Live Backup Client software to use HTTPS. To configure Live Backup Client, you must modify the Windows Registry.

WARNING

If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Atempo cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

1. On the Live Backup Client, stop all Live Backup Services and close all Live Backup applications, such as the Control Center, Recovery Wizard, etc.
2. Run the Windows Registry Editor: Click **Start**, and then click **Run**. Type **regedit**, and then click **OK**.
3. Navigate to the following key: **HKLM\SOFTWARE\Atempo\LiveBackup**
4. Edit the value **ControlUrl** (case sensitive) and replace "HTTP" with HTTPS", and replace the port assignment "80" with "443". If the key does not exist, then create it with the value as in the example, **https://servername:443/wlb/default.asp?server=(local)**
5. Edit the value of **IIServer** to include the port 443. For example, Live Backup_servername:443
6. Edit the value of **ServerName** to include the port 443. For example, Live Backup_servername:443
7. If the client computer is running Internet Explorer 7.0, you must also add the following registry key:

HKKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings

Key type: DWORD

Key name: CertificateRevocation

Key value: 0

8. Exit Registry Editor.
9. Reboot the Live Backup Client computer.
10. Upon reboot the client should connect to Live Backup Server via SSL. You can check this connection in the Network page of the Control Panel.

If the client fails to connect, contact Atempo Technical Support. Atempo Support hours are 6:00 AM to 6:00 PM PST Monday through Friday (except major U.S. holidays) via livesupport@Atempo.com or (310) 302-7285. Outside of North America, please contact your distributor or Atempo directly at intllivesupport@atempo.com.