

Engineering Advisory 52609

Mutual Transport Layer Security Provisioning Using Microsoft[®] Internet Information Services 6.0

This engineering advisory explains how to configure Microsoft[®] Internet Information Services (IIS) and Microsoft Certificate Authority to provision a Polycom[®] SoundPoint[®] IP, SoundStation[®] IP, or VVX[™] phone using mutual Transport Layer Security (mutual TLS).

This information applies to Microsoft IIS 6.0 on Windows Server[®] 2003 and the following Polycom phones:

- SoundPoint IP running SIP software version 3.2 or later
- SoundStation IP running SIP software version 3.2 or later
- VVX 1500 running SIP software version 3.2 or later
- VVX 500 running UC software version 4.1.0B or later
- VVX 600 running UC software version 4.1.2 or later

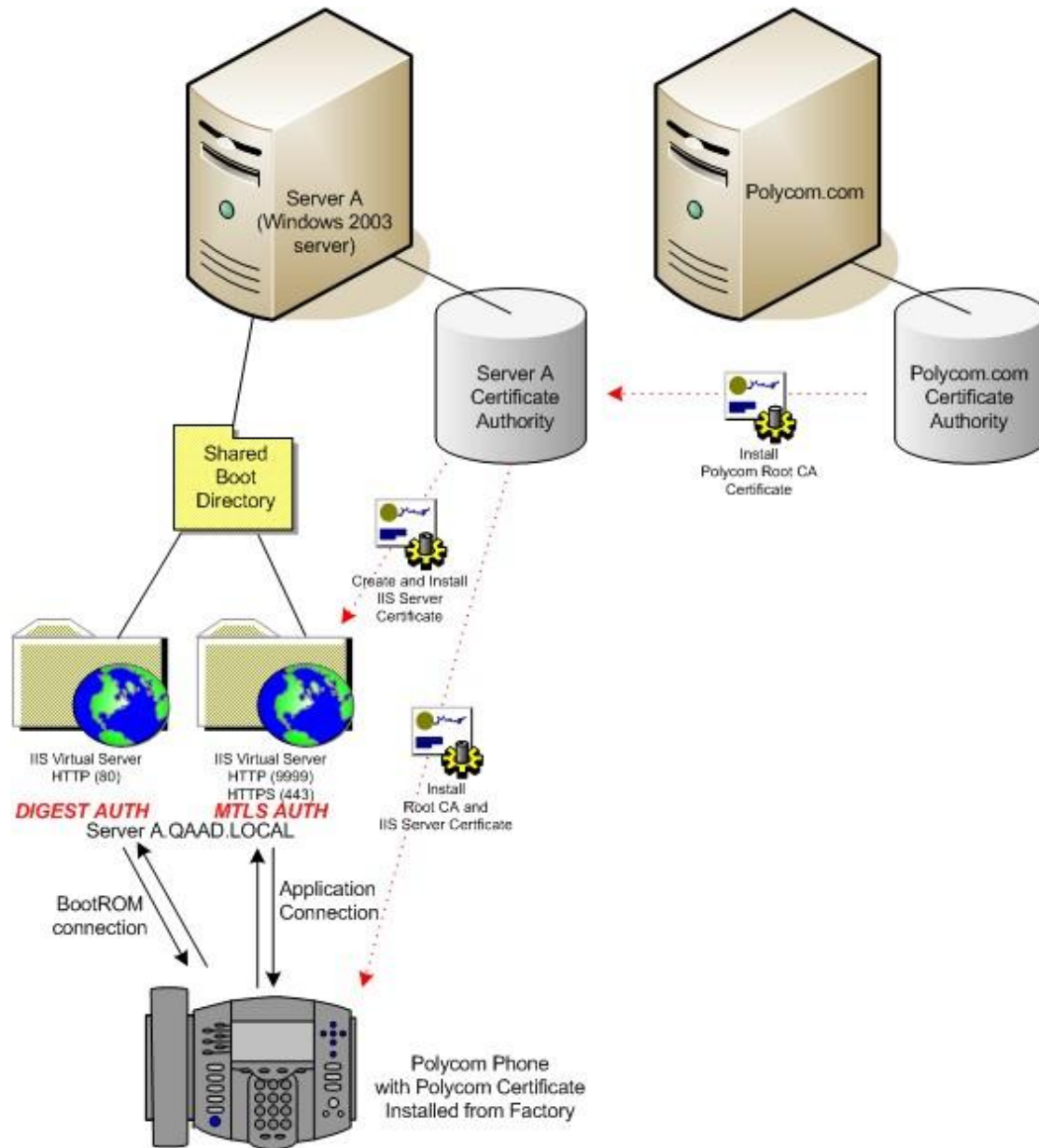
The topics in this advisory include:

- [Overview](#) A graphical overview of the configuration.
- [Mutual TLS Requirements](#) Requirements before you start the configuration.
- [Configuring Mutual TLS Provisioning](#) Procedures to show you how to configure IIS and Microsoft Certificate Authority to provision a Polycom phone using mutual TLS.
- [Troubleshooting](#) Tips to help you troubleshoot configuration problems.
- [Additional Information](#) More information on HTTP and HTTPS provisioning.

Overview

In the following figure, IIS and Microsoft Certificate Authority have been configured to provision a Polycom phone using mutual TLS. IIS is configured to allow both HTTP and mutual TLS to co-exist on a single server.

Figure 1: A Polycom Phone Using Mutual TLS and Provisioned with Configured Microsoft IIS and Microsoft Certificate Authority





Note: Purchasing a Certificate

You can simplify the configuration by purchasing a certificate for your IIS server from a well-known certificate authority (CA) instead of running the Microsoft Certificate Authority service.

Mutual TLS Requirements

Before you can configure Microsoft IIS and Microsoft Certificate Authority to provision a Polycom phone using mutual TLS, ensure that you have the following:

- Polycom SIP application 3.2 or later for mutual TLS feature.
- Polycom bootROM 4.2.0 or later for MD5 digest HTTP authentication.
- Web server capable of mutual TLS (client certificate checking). For the configuration example in this bulletin, IIS is used.
- One of the following:
 - HTTPS server certificate and root CA certificate if it is self-signed, or
 - A certificate from VeriSign® or another well-known root CA.
- Polycom phone with a certificate installed at the factory.

To verify that the certificate is installed, on the Polycom phone, press the **Menu** button, and then select **Status > Platform > Phone**. If a certificate is installed, “Device Certificate: Installed” will be listed. If a certificate is not installed, “Device Certificate: Not Installed” will be listed.

- [Polycom Root CA certificate](#)
- Patch for Microsoft server to use SHA2 256 or higher encryption. For more information, see the related entry in the [Troubleshooting](#) section.

Configuring Mutual TLS Provisioning

The procedures in this section show you how to configure IIS and Microsoft Certificate Authority to provision a Polycom phone using mutual TLS.

Configuring mutual TLS provisioning involves the following steps:

- 1 [Creating a Directory on the IIS Server](#)
- 2 [Creating the HTTP Virtual Server in IIS](#)

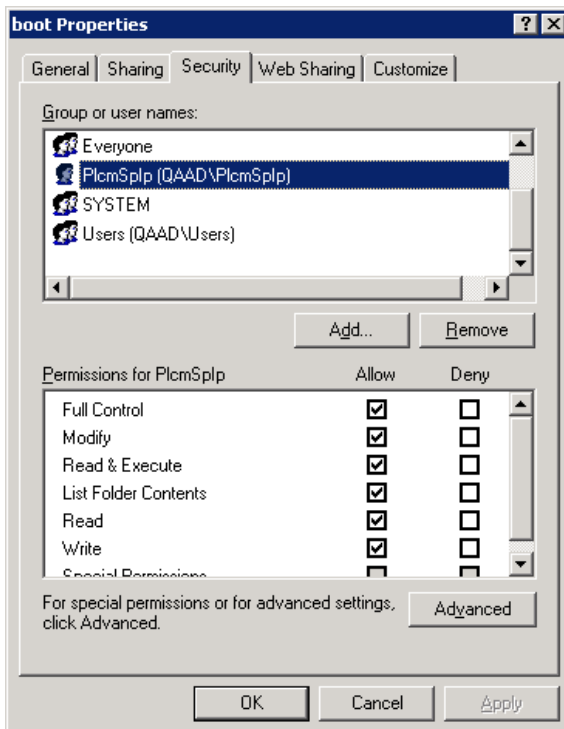
- 3 [Creating the HTTPS Virtual Server in IIS](#)
- 4 [Installing Microsoft Certificate Service](#)
- 5 [Creating the IIS Server Self-Signed Certificate for the IIS HTTPS Server](#)
- 6 [Installing the Server Certificate on the IIS Server](#)
- 7 [Installing the Root CA Server Certificate on the Polycom Phone](#)
- 8 [Installing the Polycom Root CA Certificate on the Microsoft Certificate Authority Server](#)
- 9 [Enabling Mutual TLS on the IIS Server](#)

Creating a Directory on the IIS Server

Create a directory on the IIS Server to contain the boot files for the Polycom phone.

To create a directory on the IIS Server:

- 1 Create a folder (boot directory) on the IIS server and place all the phone's boot files in the directory. (You will configure the IIS server to point to this directory in a later step.)
- 2 Create a user account for the phone and provide **Full Control** access to the boot directory. If there is a problem with permissions to files, add the "Everyone" group and give it **Full Control** access.

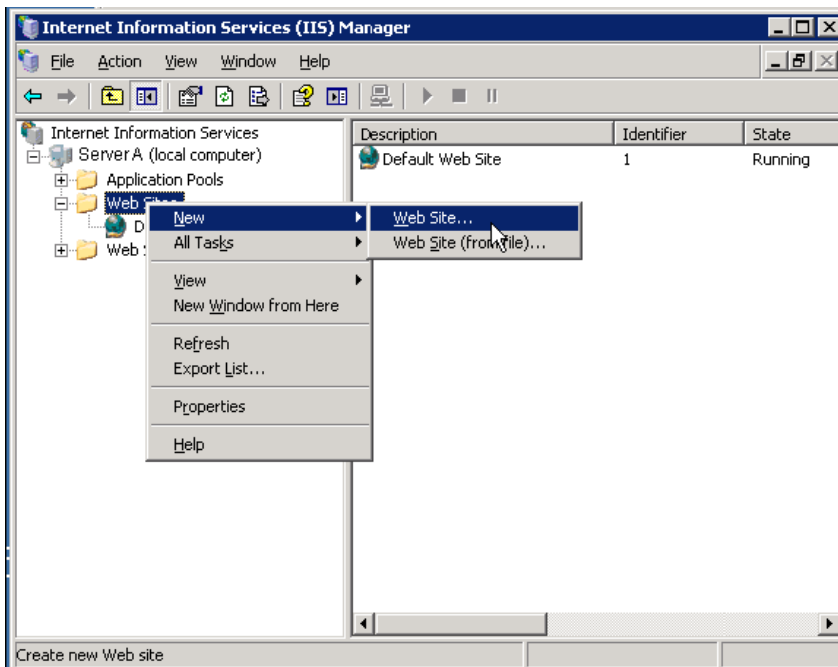


Creating the HTTP Virtual Server in IIS

Create the HTTP virtual server in IIS for the bootROM bootup.

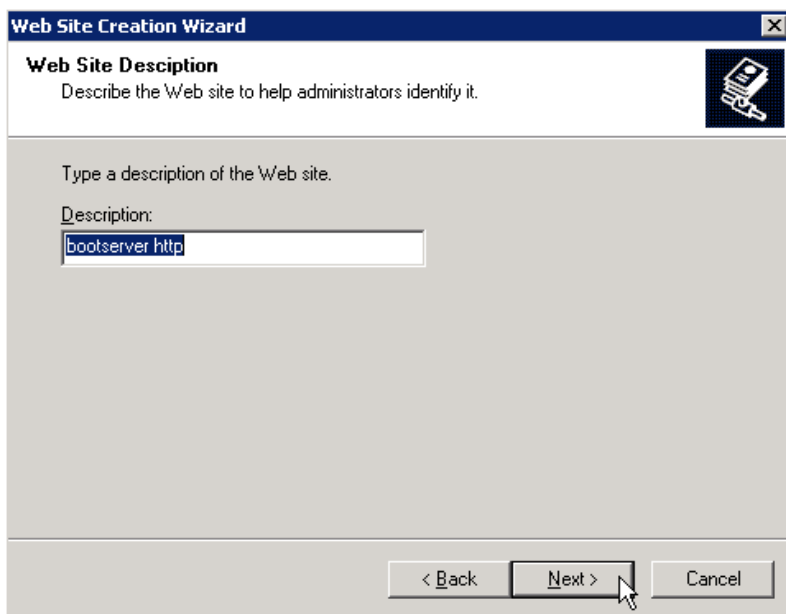
To create the HTTP virtual server:

- 1 Open Internet Information Services (IIS) Manager. Right-click **Web Sites**, and then select **New > Web Site**.

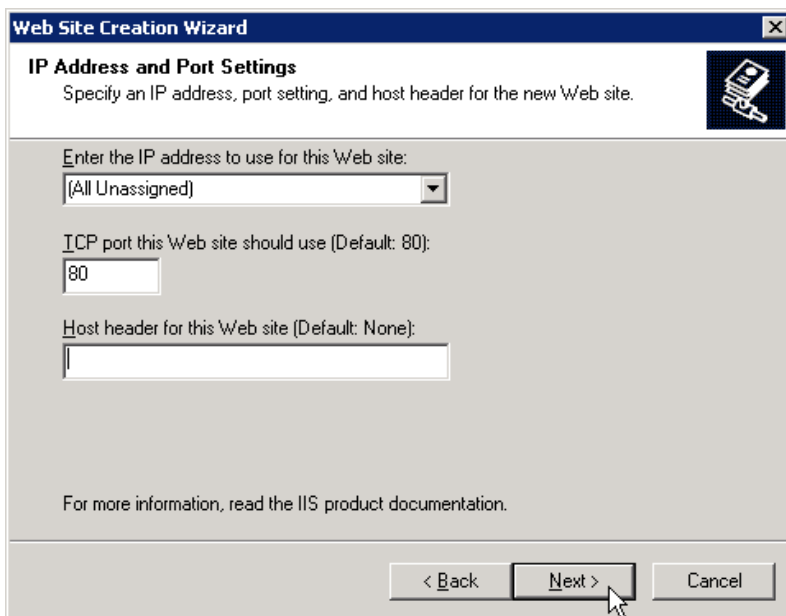


2 From the Web Site Creation Wizard, do the following:

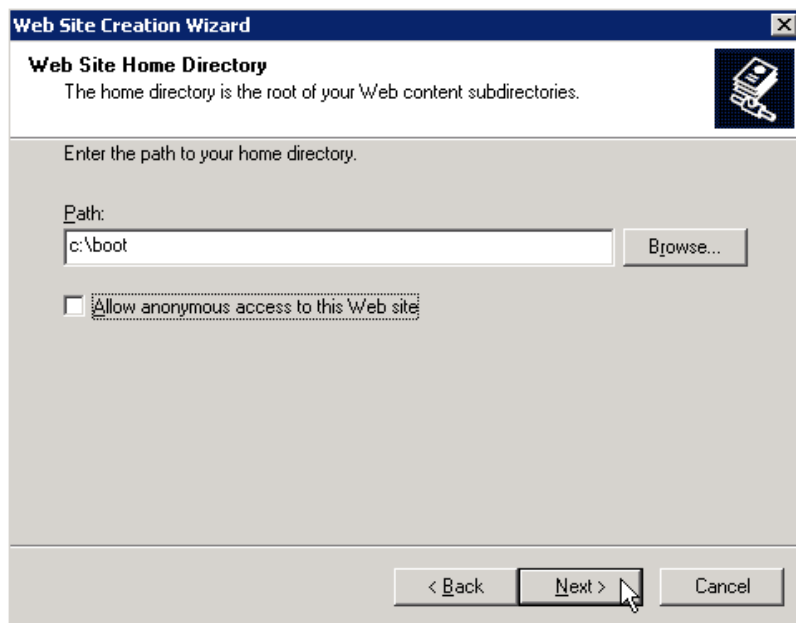
- a In the **Description** box, enter the name of the virtual server (for example, **bootserver http**), and then click **Next**.



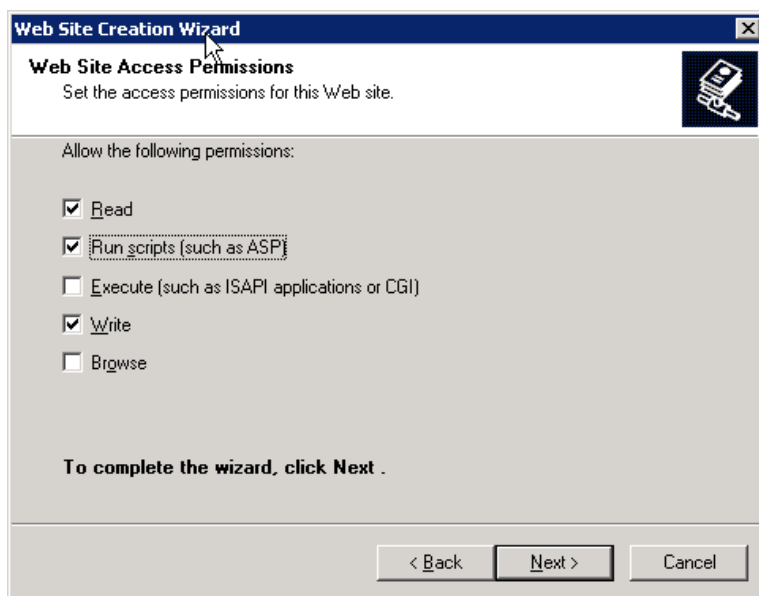
- b In the **TCP port this Web site should use** box, enter **80**, and then click **Next**.



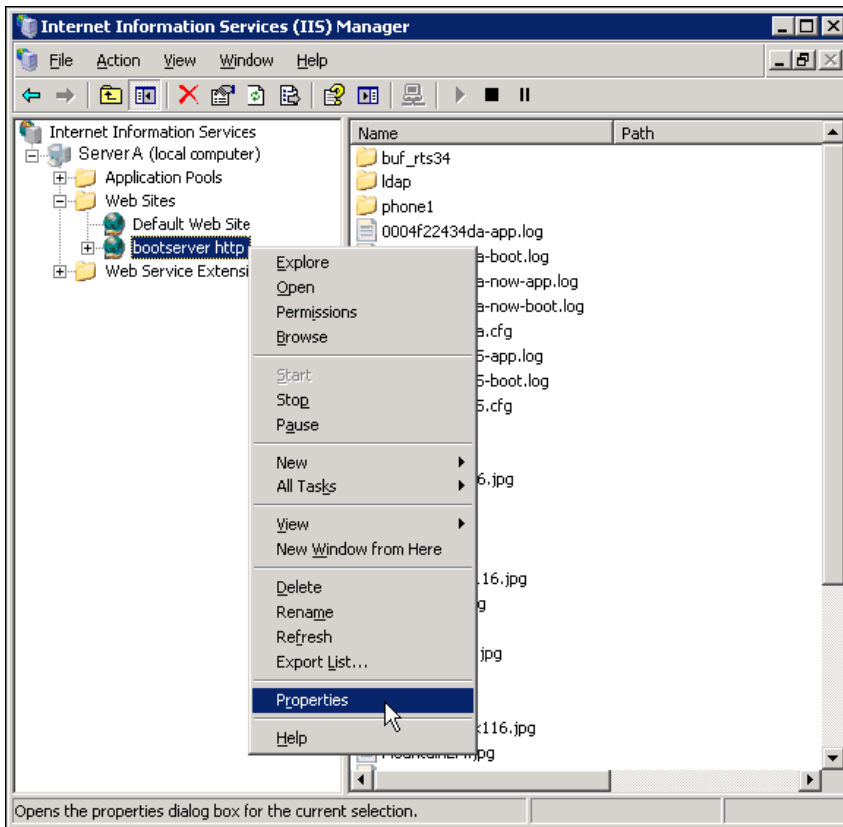
- c In the **Path** box, enter the name of the boot directory you created as the home directory, and then clear the **Allow anonymous access to this Web site** check box to secure the virtual server. Then click **Next**.



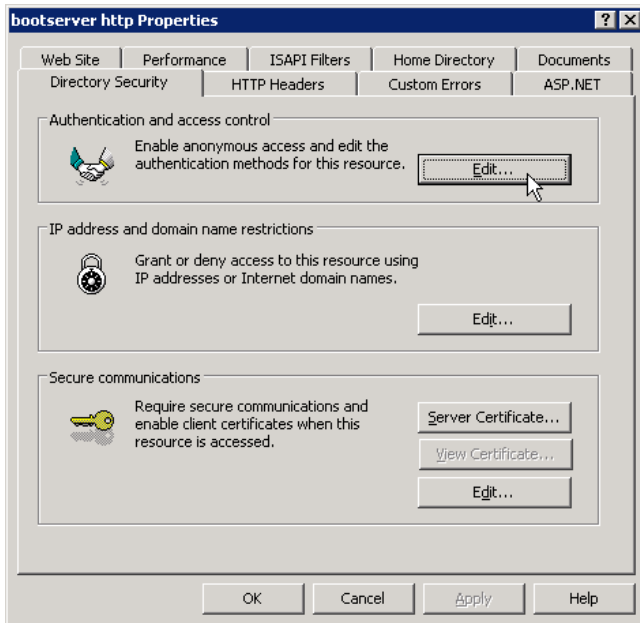
- d Select the **Read**, **Run scripts (such as ASP)**, and **Write** check boxes, and then click **Next**. (You require write access for logs, and you need to run scripts so you can download certificates.)



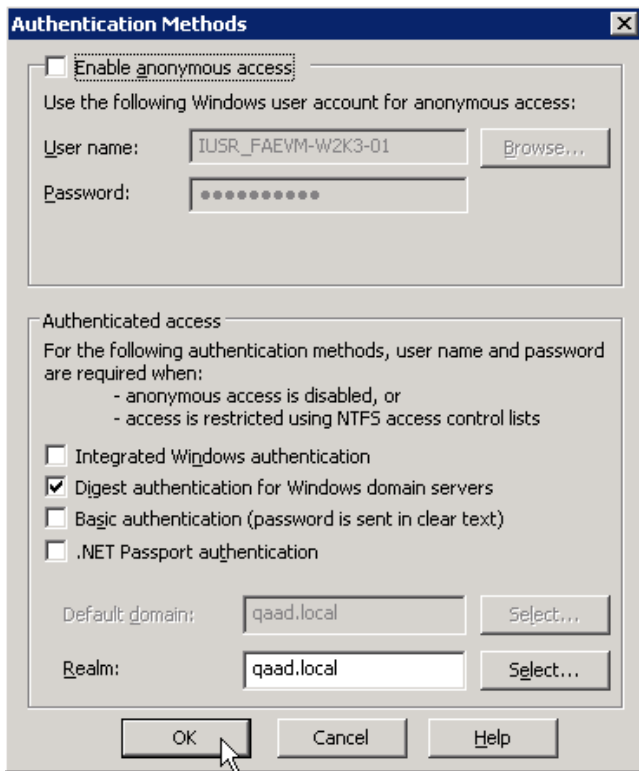
- 3 From the Internet Information Services (IIS) Manager window, right-click the virtual server (for example, **bootserver http**), and then select **Properties**.



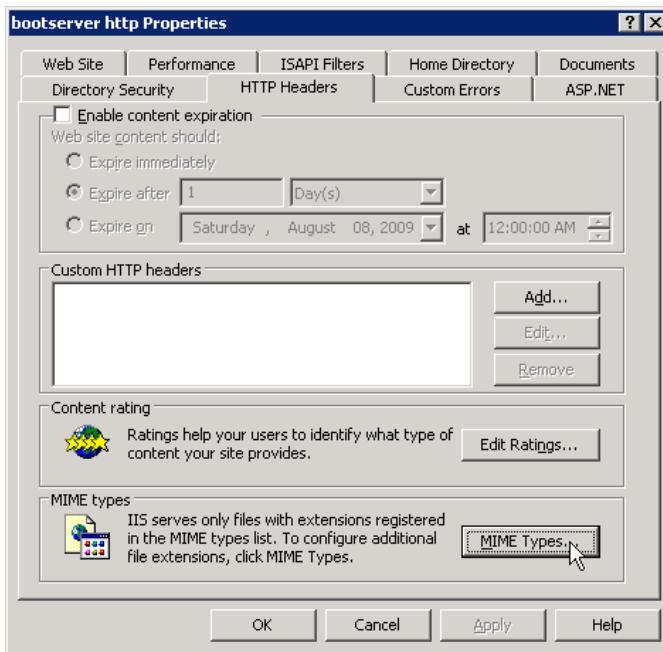
- 4 From the <virtual server name> Properties window, click the **Directory Security** tab. Then, in the **Authentication and access control** area, click **Edit**.



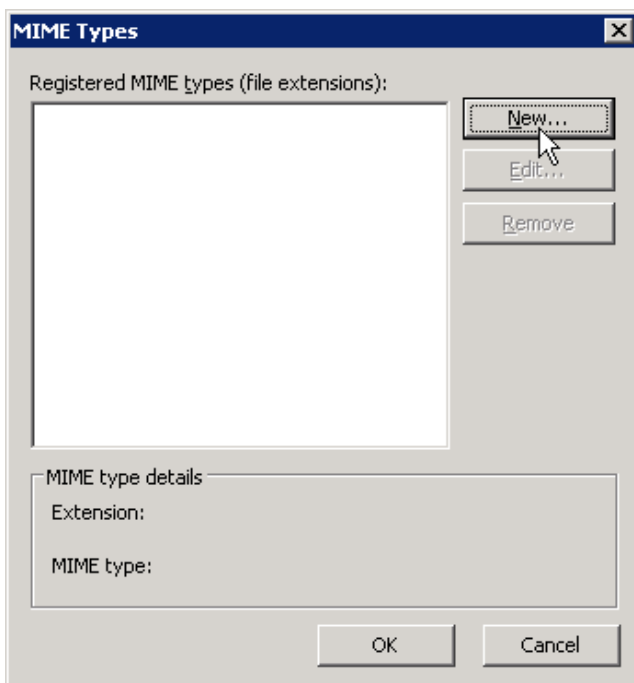
- 5 From the Authentication Methods window, clear all the check boxes, except the **Digest authentication for Windows domain servers** check box, and then click **OK**. (Digest Authentication requires Active Directory and a domain user account.)



- 6 From the <virtual server name> Properties window, click the **HTTP Headers** tab. Then, in the **MIME types** area, click **MIME Types**.



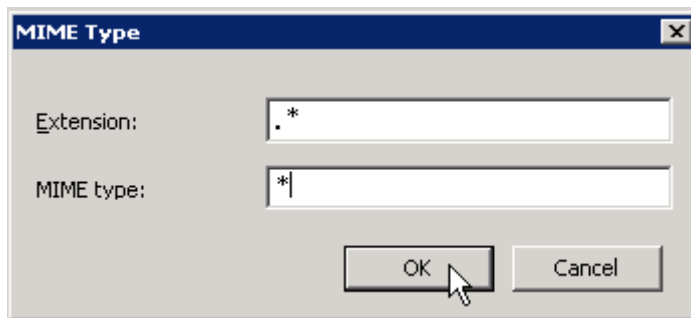
- 7 From the MIME Types window, click **New**.



8 From the MIME Type window, do the following:

- a** In the **Extension** box, enter *.*
- b** In the **MIME type** box, enter *
- c** Click **OK**.

These settings allow the phone to download everything in the boot directory (for example, .cfg and .ld).

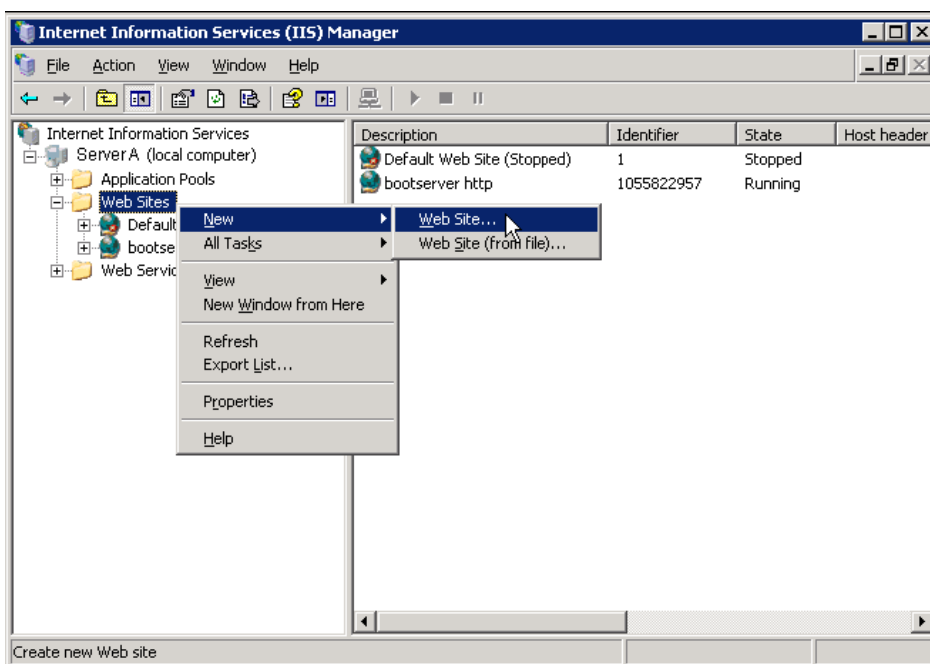


Creating the HTTPS Virtual Server in IIS

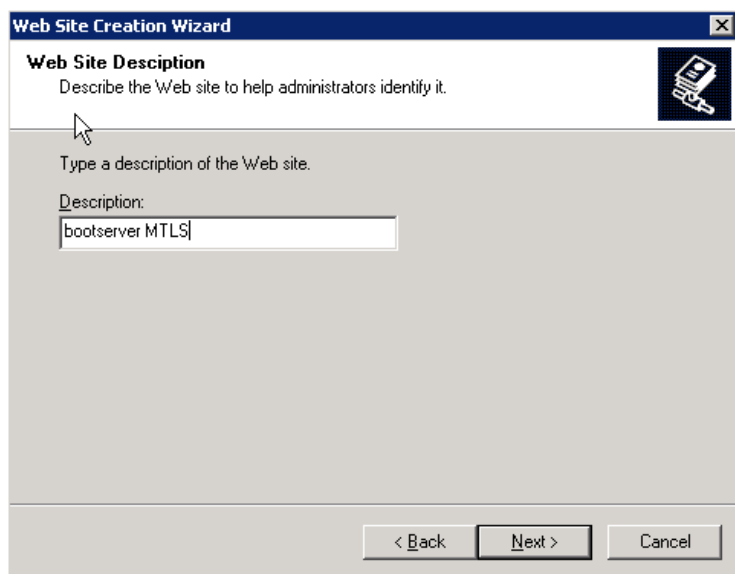
Create the HTTPS virtual server in IIS for the application bootup. You need to create a second server because after you enable mutual TLS on the virtual server, the HTTP portion of the virtual server becomes inactive.

To create the HTTPS virtual server:

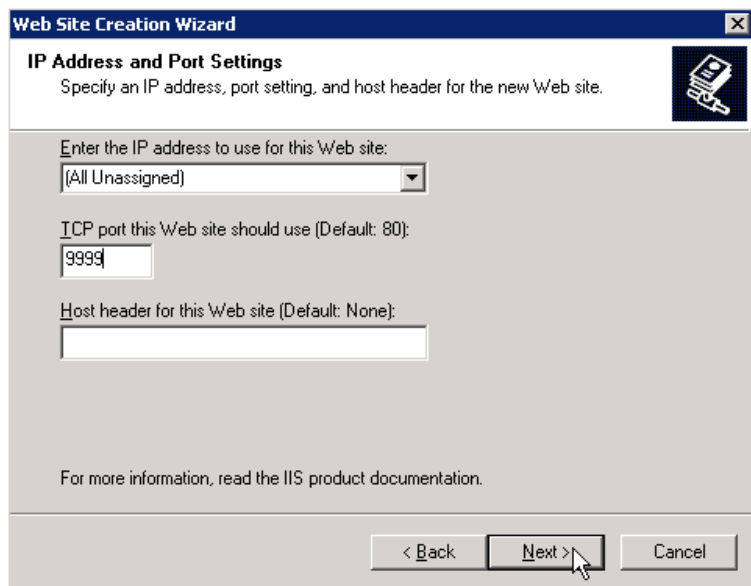
- 1 Open Internet Information Services (IIS) Manager. Right-click **Web Sites**, and then select **New > Web Site**.



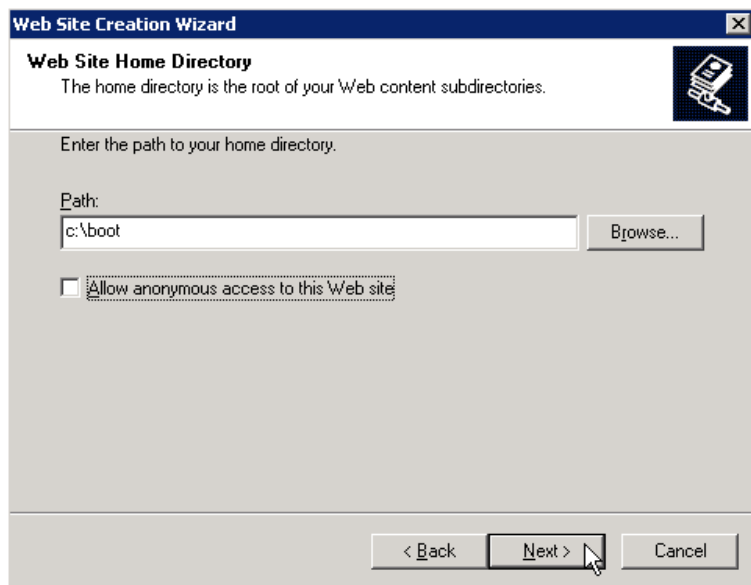
- 2 From the Web Site Creation Wizard, do the following:
 - a In the **Description** box, enter a name for the virtual server (for example, **bootserver MTLs**), and then click **Next**.



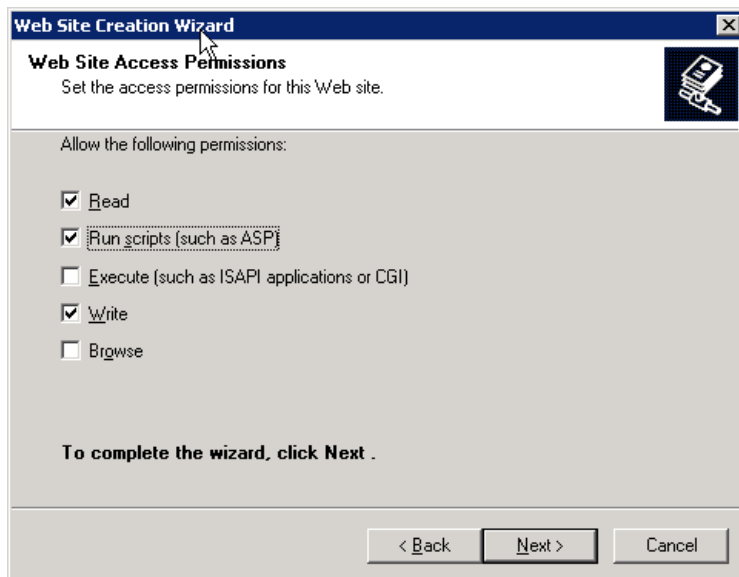
- b** In the **TCP port this Web site should use** box, change the port to an unused port (for example, 9999). This port will be disabled when mutual TLS for this virtual server is enabled in a later step. Then click **Next**.



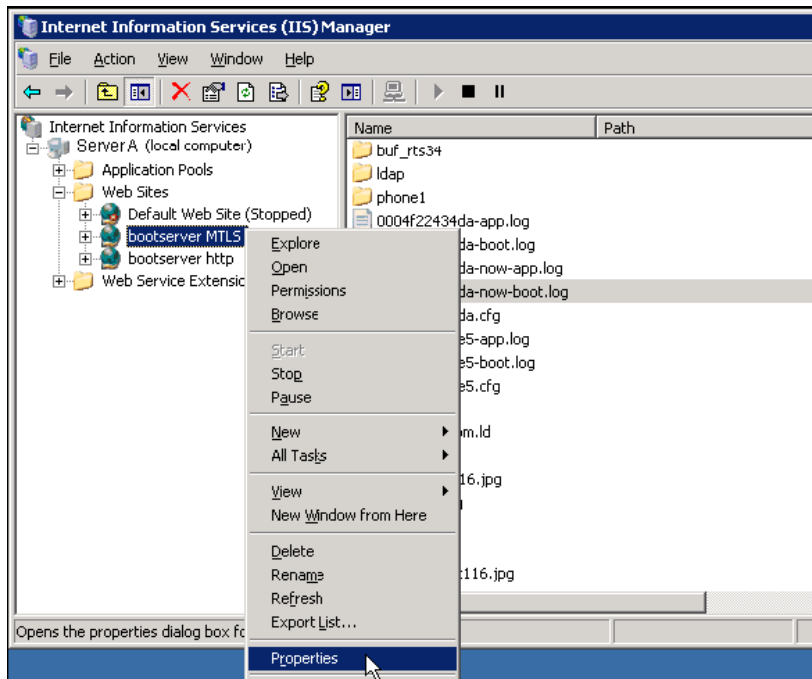
- c** In the **Path** box, enter the location of the boot directory (it can be the same directory as the boot directory you specified in the previous section), and then clear the **Allow anonymous access to this Web site** check box to secure the virtual server. Then click **Next**.



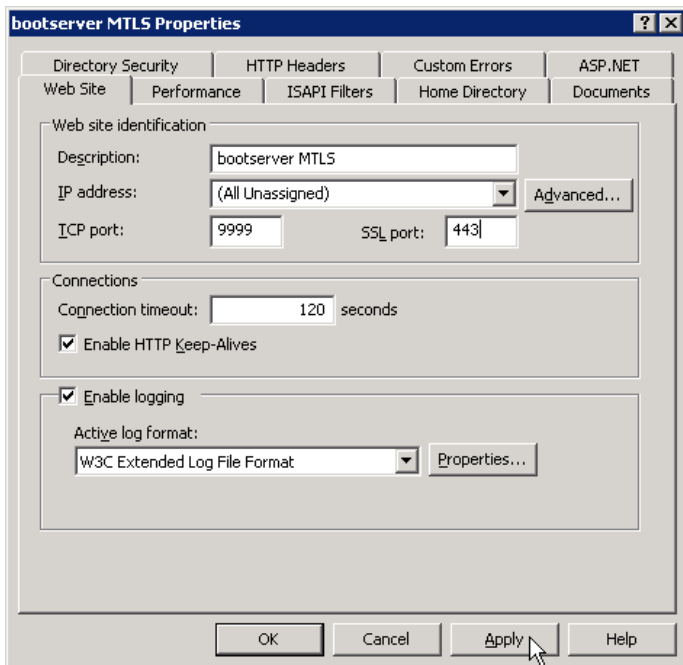
- d Select the **Read**, **Run scripts (such as ASP)**, and **Write** check boxes, and then click **Next**.



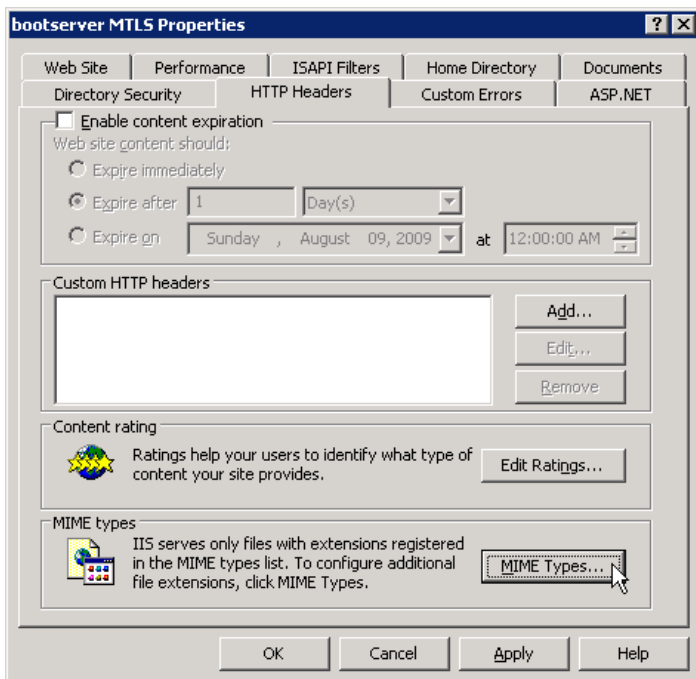
- 3 From the Internet Information Services (IIS) Manager window, right-click the virtual server (for example, **bootserver MTL5**), and then select **Properties**.



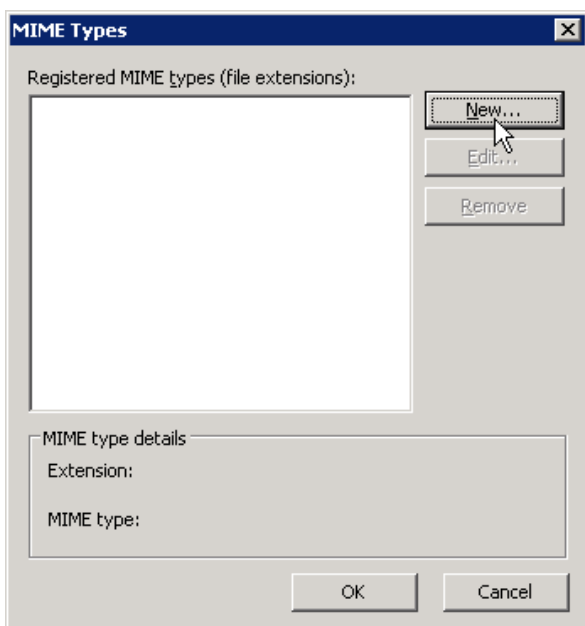
- 4 From the <virtual server name> Properties window, click the **Web Site** tab. In the **Web site identification** area, enter **443** in the **SSL port** box. Click **Apply**.



- 5 Click the **HTTP Headers** tab. In the **MIME types** area, click **MIME Types**.



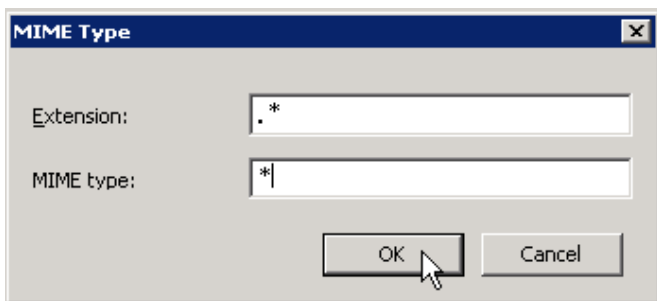
6 From the MIME Types window, click **New**.



7 From the MIME Type window, do the following:

- a In the **Extension** box, enter **.***
- b In the **MIME type** box, enter *****
- c Click **OK**.

These settings allow the phone to download everything in the boot directory (for example, .cfg and .ld).



There are now two functioning IIS virtual web servers (HTTP and HTTPS).

8 At the command prompt, type **IISRESET** to restart the web servers.

Installing Microsoft Certificate Service

Skip this section if you are using a certificate from a well-known certificate authority such as VeriSign®. If you plan to run your own certificate authority, complete the steps in this section.

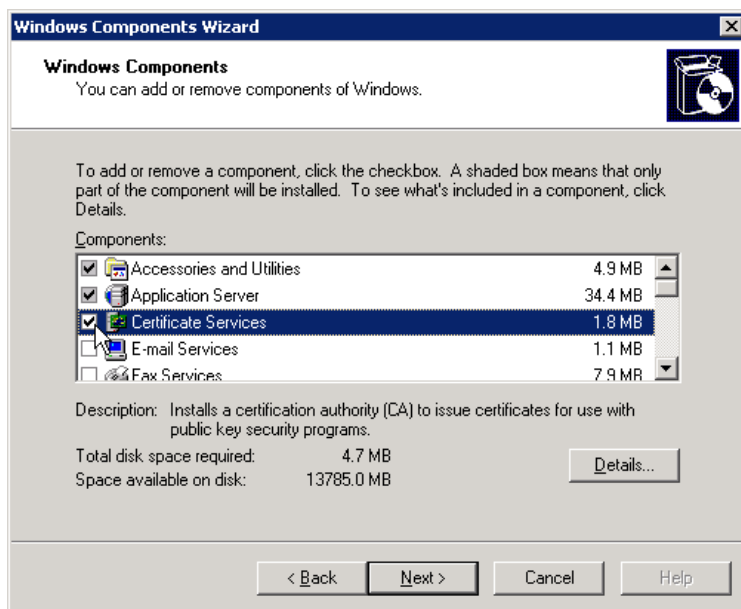


Note: Provisioning Server Running Active Directory

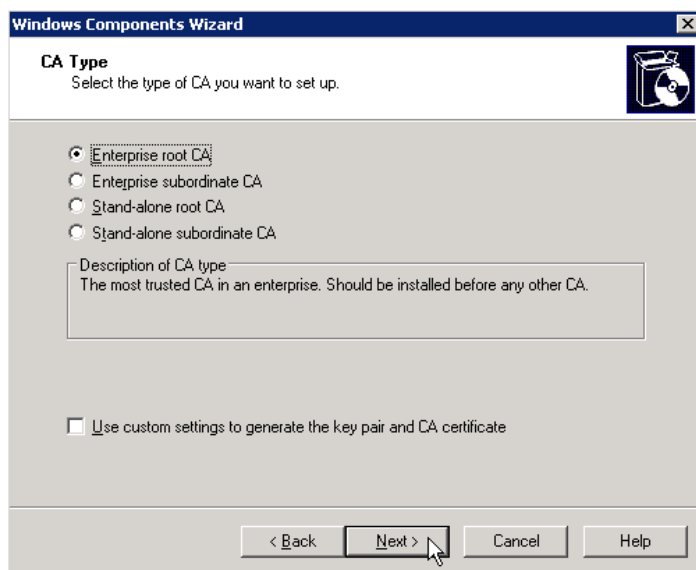
Before you complete the steps in this section, make sure your provisioning server is running or part of an Active Directory.

To install Microsoft Certificate Services:

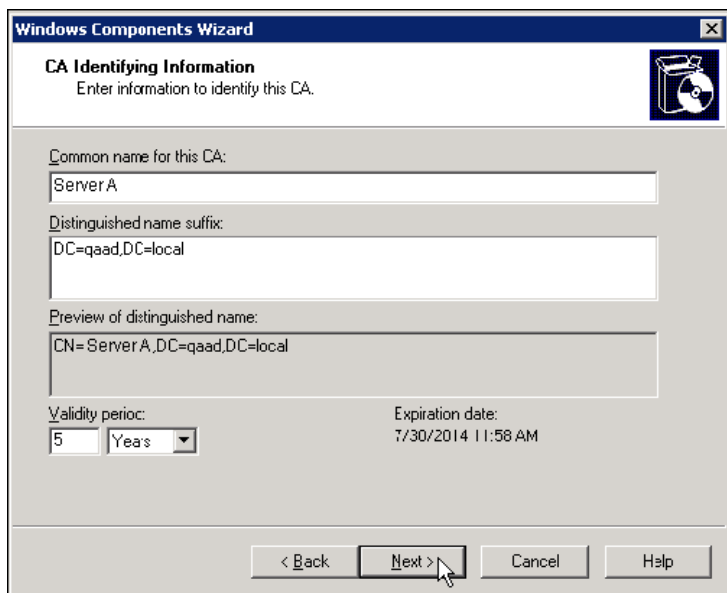
- 1 In Control Panel, double-click **Add or Remove Programs**. Then, click **Add/Remove Windows Components**.
- 2 From the Windows Components Wizard window, do the following:
 - a Select the **Certificate Services** check box, and then click **Next**.



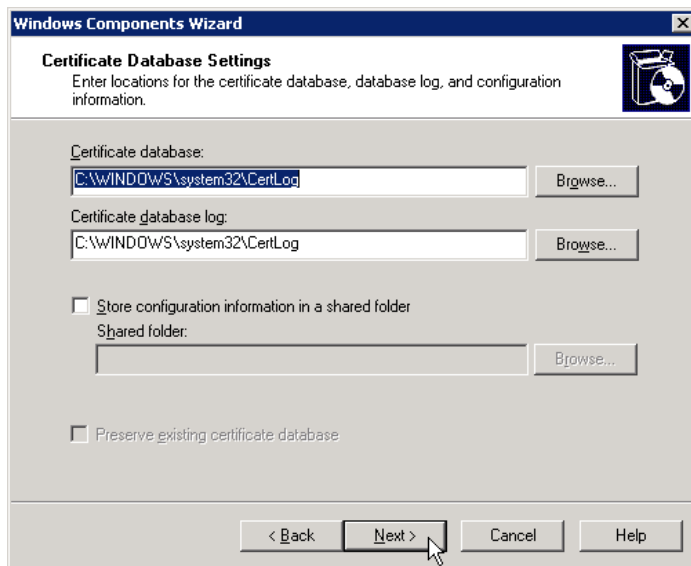
- b Select **Enterprise root CA** (assuming the server is running Active Directory), and then click **Next**.



- c In the **Common name for this CA** box, enter the common name for your certificate authority (for example, the server name), and then click **Next**.



- d In the **Certificate database** and **Certificate database log** boxes, enter the default file locations for the certificate database and database log, and then click **Next**.



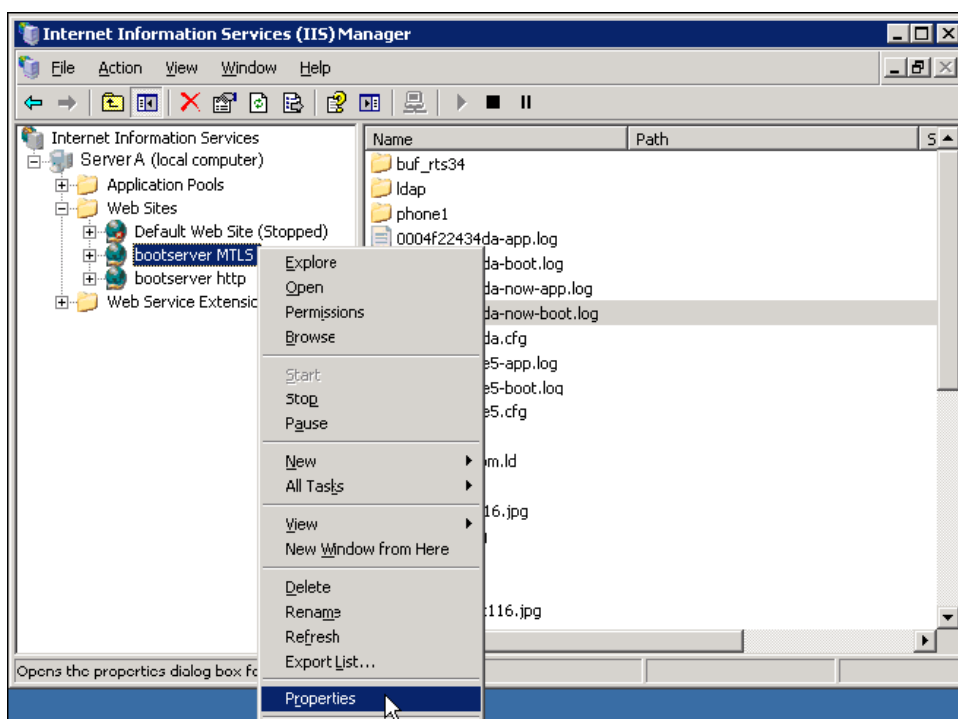
At this point, the Microsoft Certificate Authority will start to install. Microsoft Windows Media 2003 may be required to complete the installation.

Creating the IIS Server Self-Signed Certificate for the IIS HTTPS Server

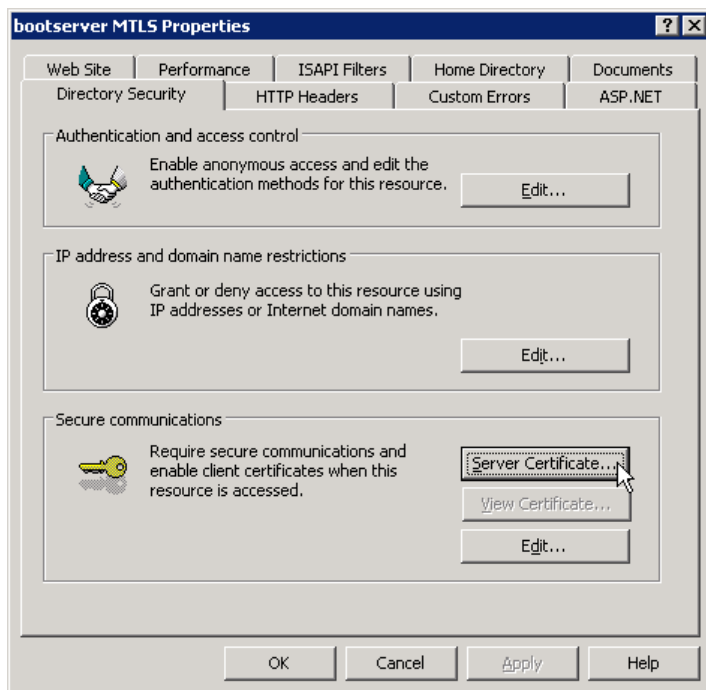
Skip this section if you are using a certificate from a well-known certificate authority such as VeriSign®. If you plan to run your own certificate authority, complete the steps in this section.

To create the IIS server self-signed certificate:

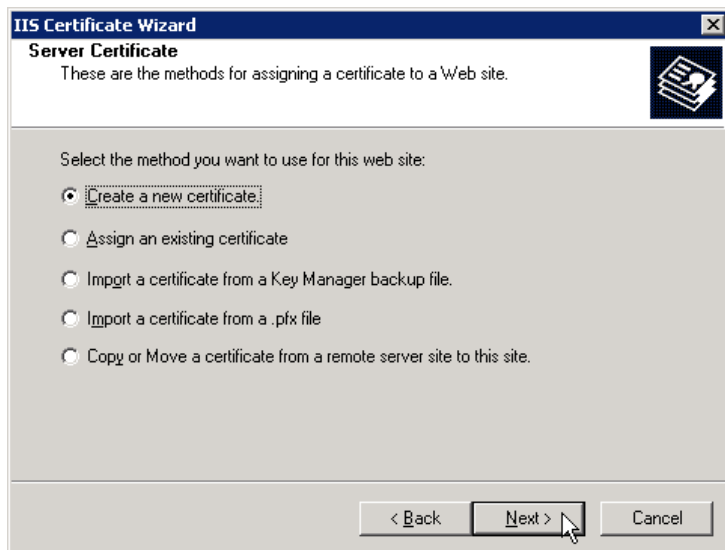
- 1 Open Internet Information Services (IIS) Manager. Right-click the HTTPS virtual server (for example, **bootserver MTLs**), and then select **Properties**.



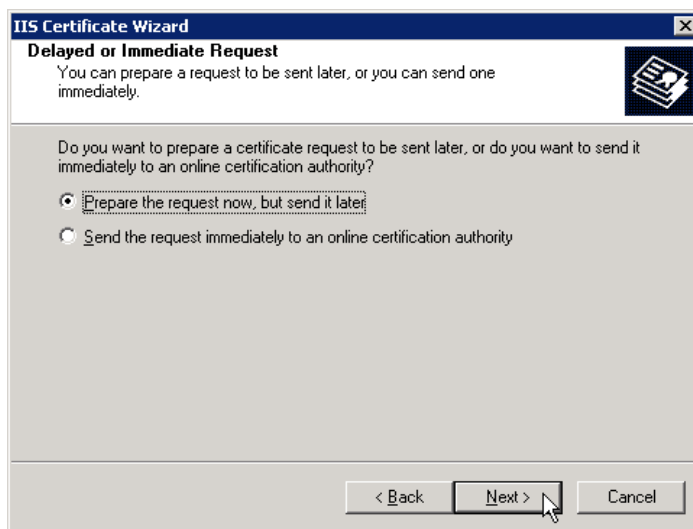
- From the <virtual server name> Properties window, click the **Directory Security** tab. In the **Secure communications** area, click **Server Certificate**.



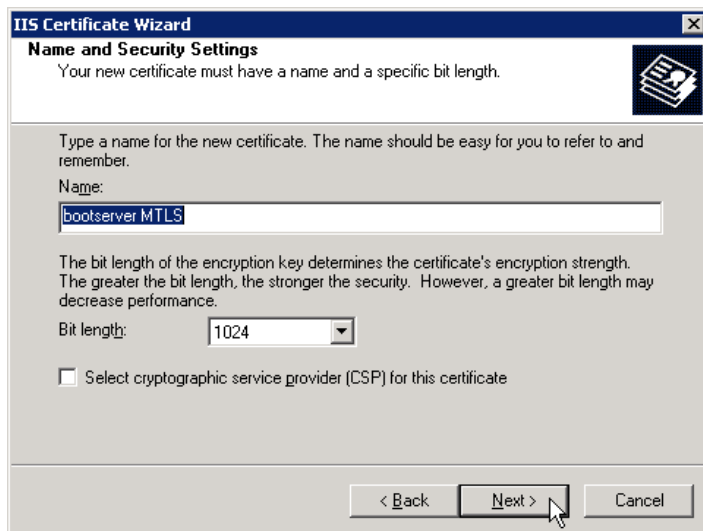
- Click **Create a new certificate**, and then click **Next**.



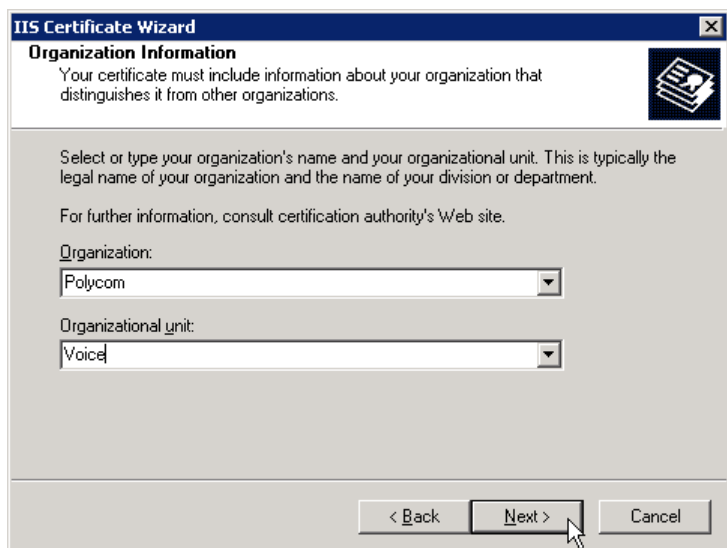
- From the IIS Certificate Wizard, do the following:
 - Click **Prepare the request now, but send it later**, and then click **Next**.



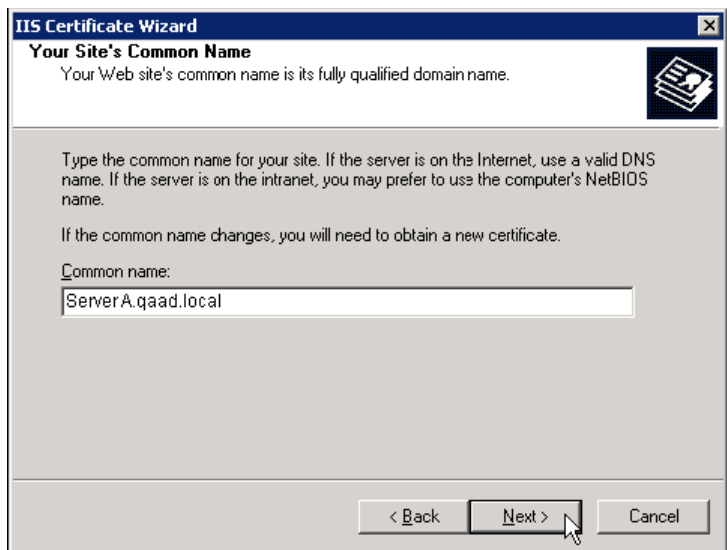
- b In the **Name** box, enter a friendly name for the certificate (for example, **bootserver MTLS**), and then click **Next**.



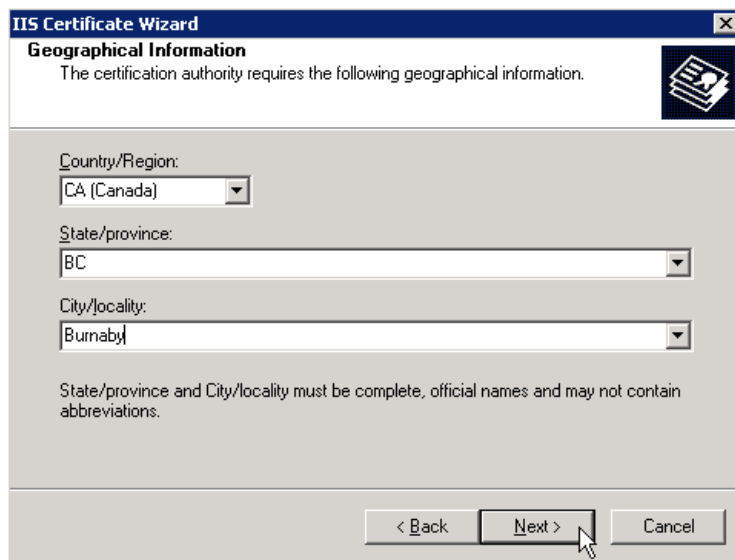
- c In the **Organization** and **Organizational unit** boxes, enter your organizational information, and then click **Next**.



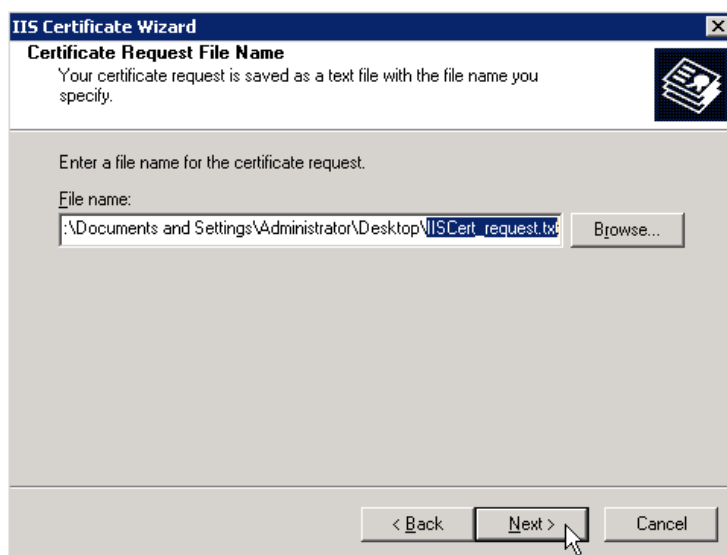
- d In the **Common name** box, enter the common name you will use to access the IIS HTTPS web server (for example, the HTTPS server's fully qualified domain name), and then click **Next**.



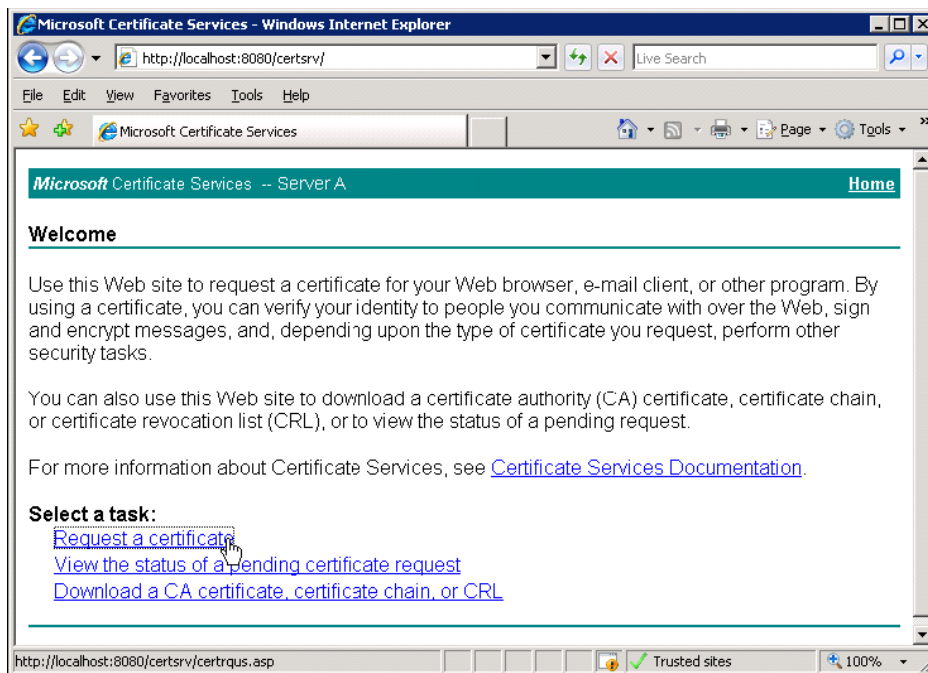
- e Enter your location information, and then click **Next**.



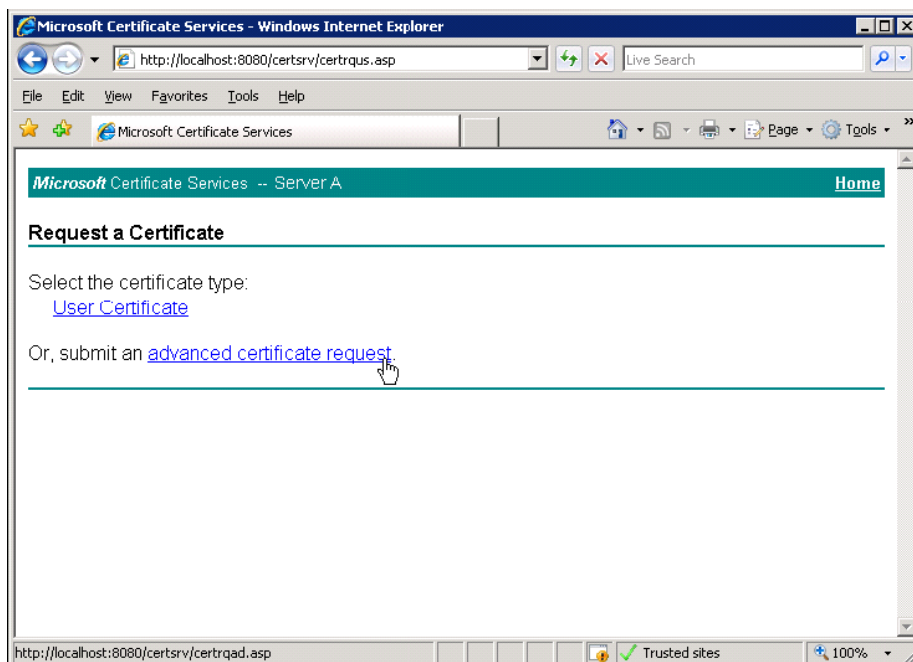
- f In the **File name** box, assign the certificate request a name you will remember, and save it to your desktop so you can access it in step 8 of this procedure. Click **Next**.



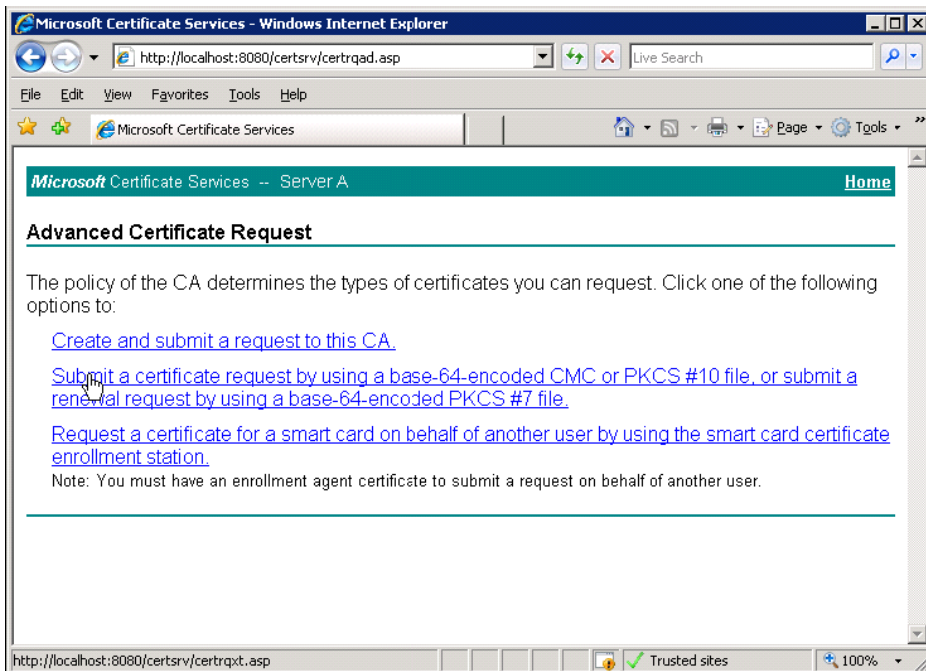
- 5 Load a web browser and go to <http://localhost/certsrv/> (the Microsoft Certificate Services web site). Under **Select a task**, click **Request a certificate**.



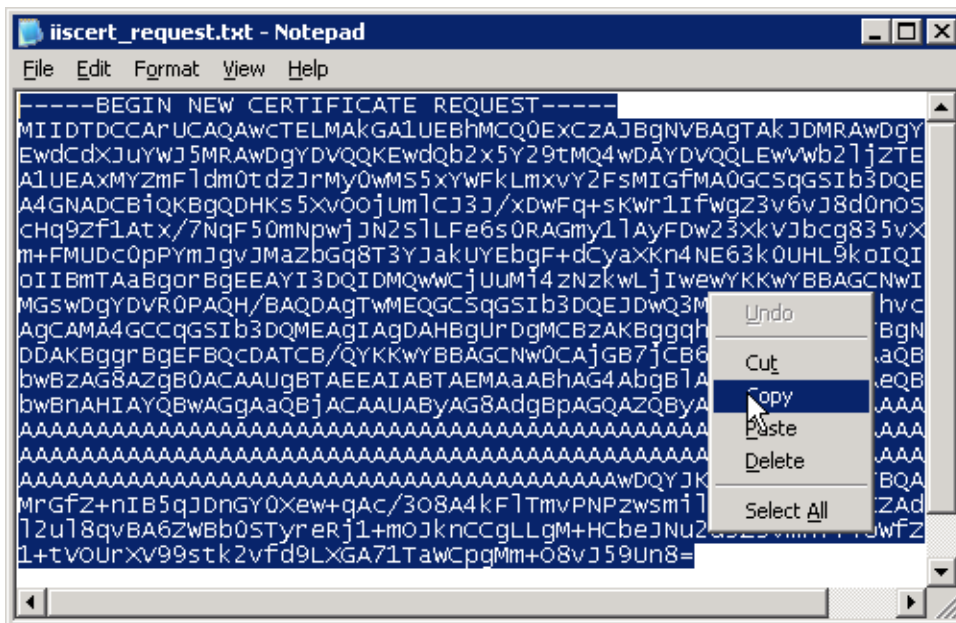
- 6 Click **advanced certificate request**.



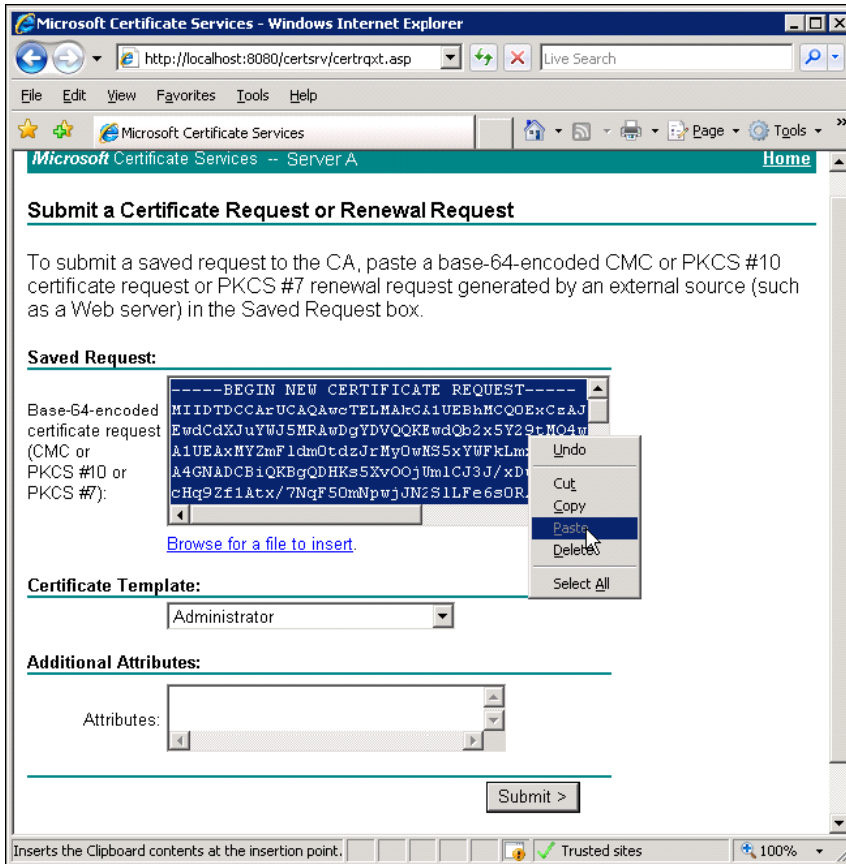
- 7 Click **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.**



- 8 In a text editor (like Notepad), open the certificate request you saved to your desktop in step 4 of this procedure, select the entire contents of the file, and then copy it to your clipboard.



9 Under **Saved Request**, paste the contents of the certificate request.



10 Under **Certificate Template**, select **Web Server**, and then click **Submit**.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDTCCArUCAQAwcTELM&kGA1UEBhMCQOExCzAJ
EwdCdXJuYWJ5MR&wDgYDVQQKEwdQb2x5Y29tMQ4w
A1UEAxMYZmFlcm0tdzJrMy0wMS5xYUFRkLmXvY2Fs
A4GNADCBiQKBgQDHKs5XvOOjUm1CJ3J/xDwFq+sK
cHq9Zf1&tx/7NqF50mNpwjJN2S1LF=6sOR&Gmy1l
```

[Browse for a file to insert.](#)

Certificate Template:

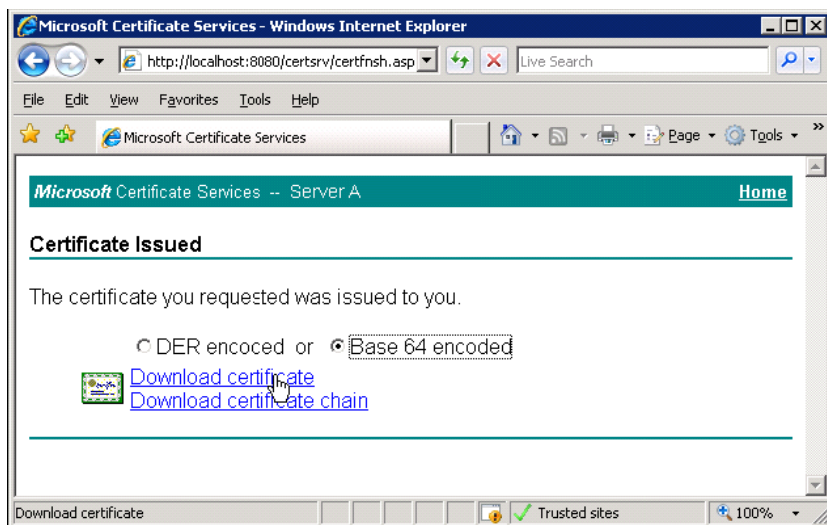
Web Server

Additional Attributes:

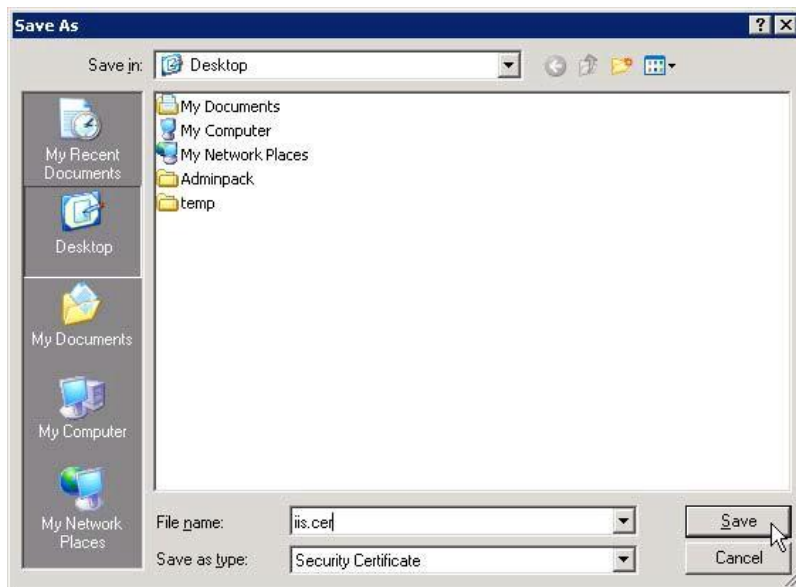
Attributes:

Submit >

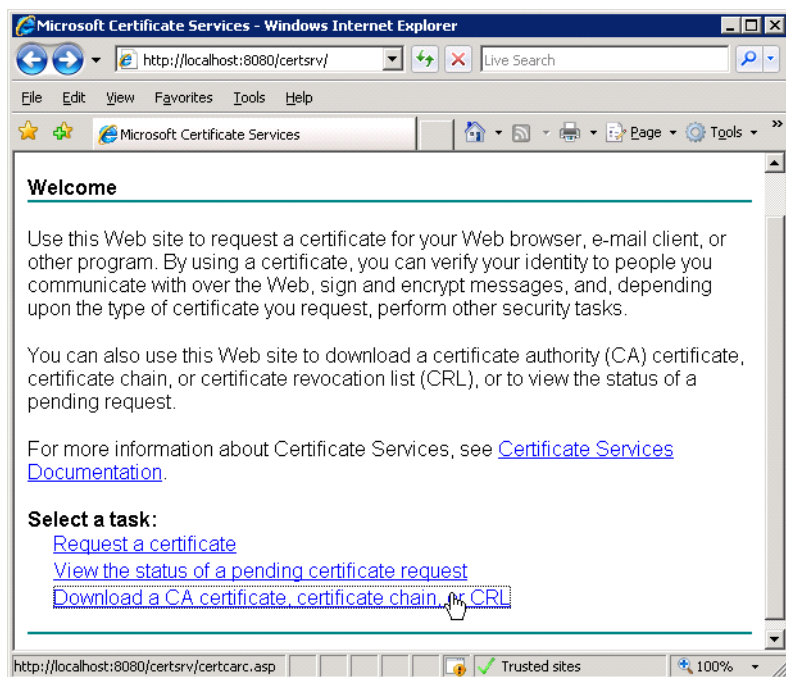
11 Click **Base 64 encoded**, and then click **Download certificate**.



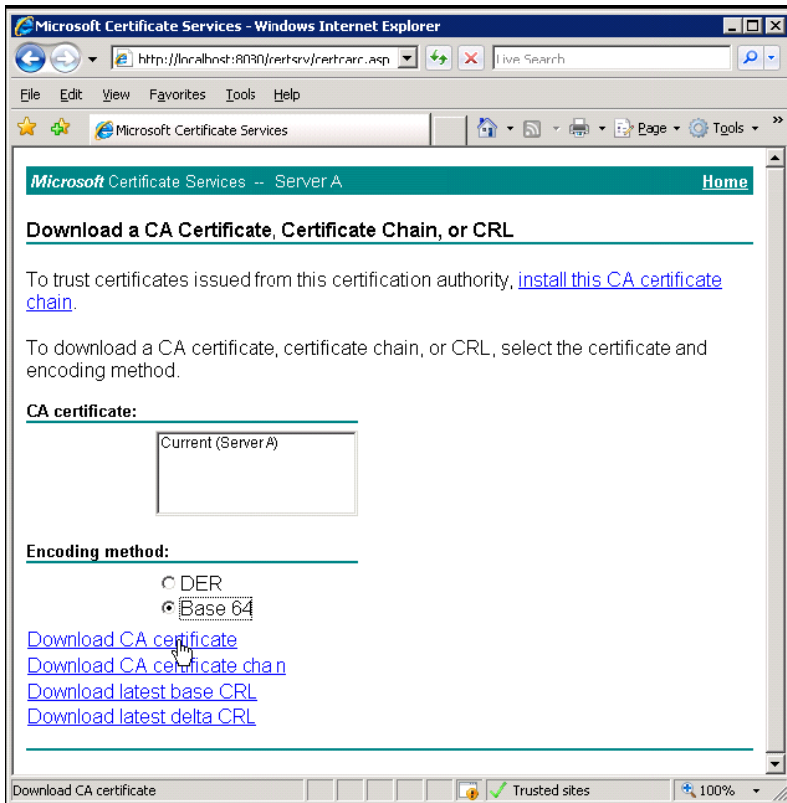
- 12 Assign the IIS server certificate a name you will remember, and then save it to your desktop so you can access it when you install the certificate on the IIS Server (see [Installing the Server Certificate on the IIS Server](#)).



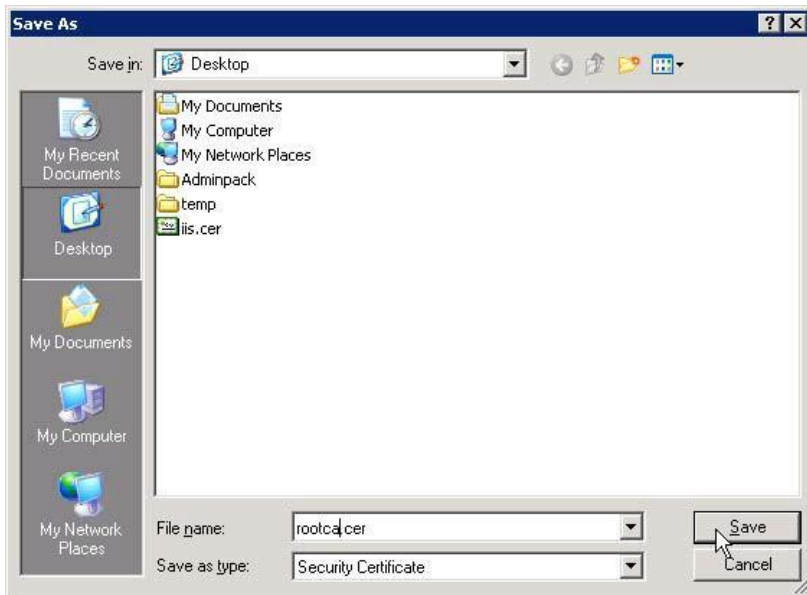
- 13 Click the Home icon to return to <http://localhost/certsrv/>, and then click **Download a CA certificate, certificate chain or CRL**.



14 Under **Encoding method**, click **Base 64**, and then click **Download CA certificate**.



- 15 Save the root CA certificate to your desktop so you can access it when you install the certificate on the Polycom phone (see [Installing the Root CA Server Certificate on the Polycom Phone](#)).



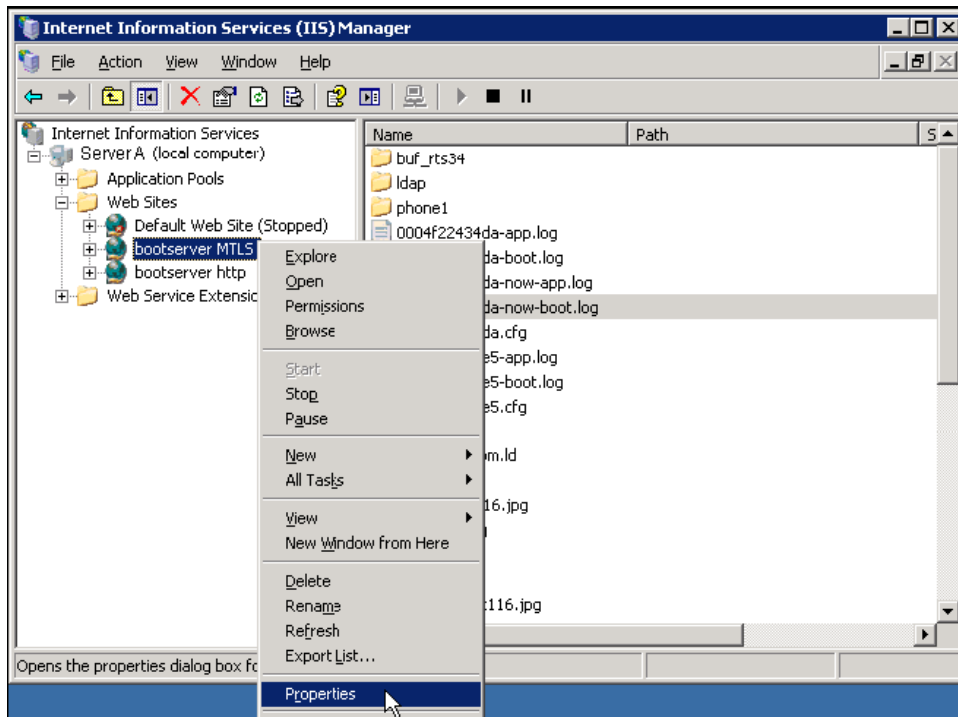
You now have two certificates saved on your desktop: the IIS server certificate and the root CA certificate.

Installing the Server Certificate on the IIS Server

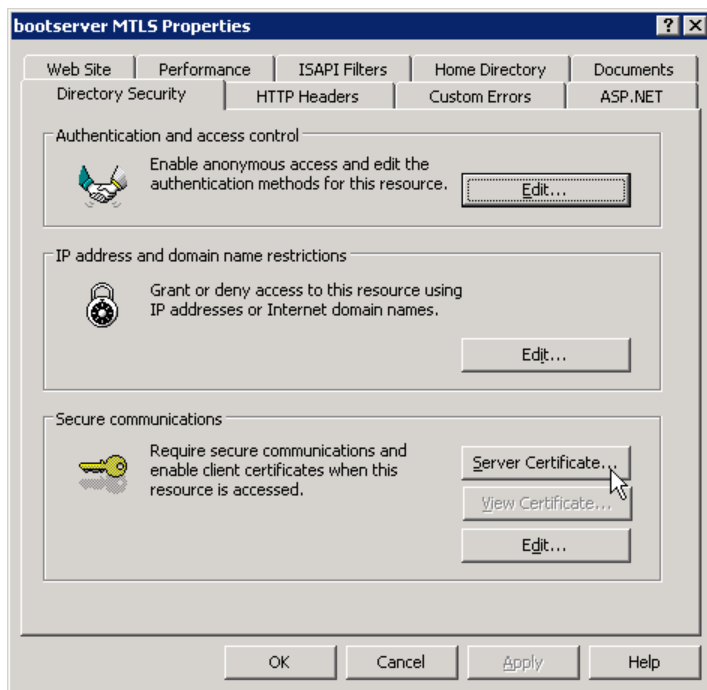
After you create the IIS server certificate for the IIS HTTPS server, install the certificate on the IIS server. If you used a certificate from a well-known certificate authority such as VeriSign®, install that certificate on the IIS server.

To install the server certificate on the IIS server:

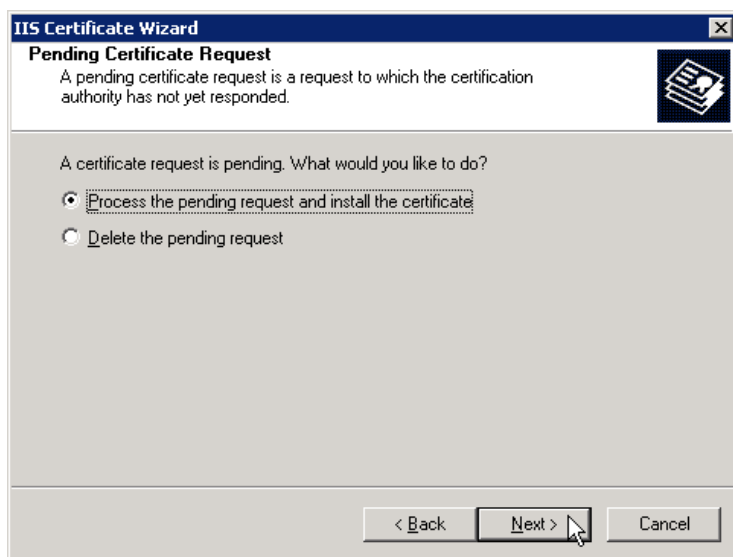
- 1 Open Internet Information Services (IIS) Manager. Right-click the HTTPS virtual server (for example, **bootserver MTLS**), and then select **Properties**.



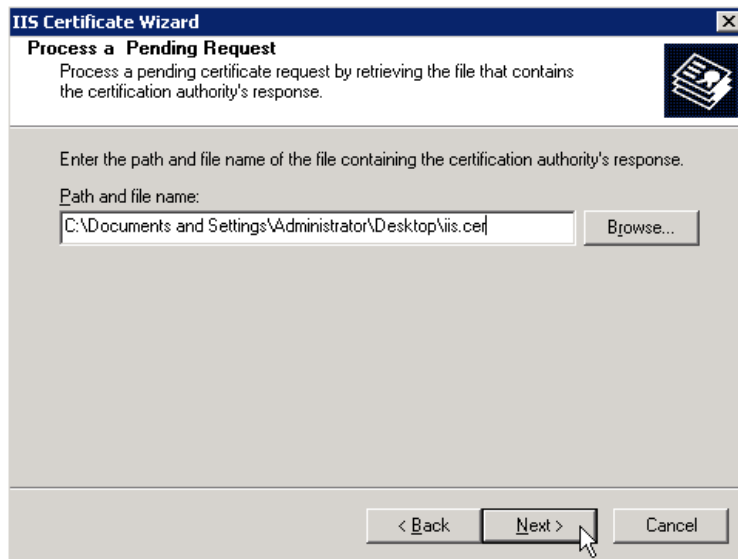
- 2 From the <virtual server name> Properties window, click the **Directory Security** tab. In the **Secure communications** area, click **Server Certificate**.



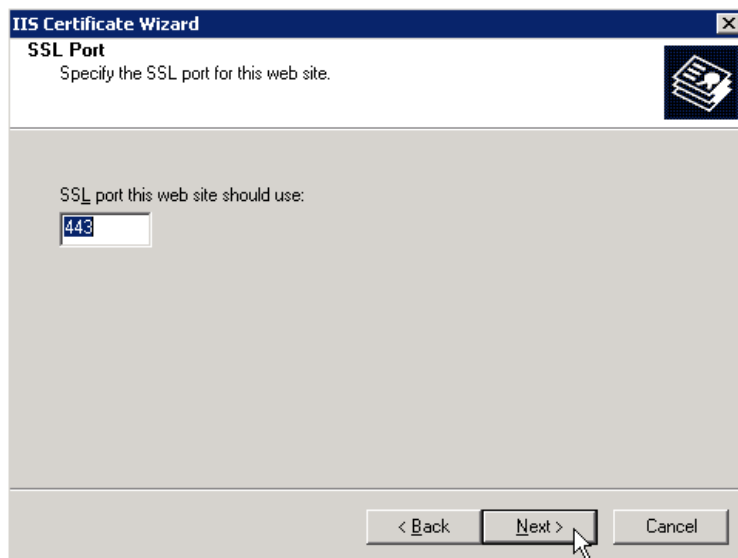
- 3 From the IIS Certificate Wizard window, do the following:
 - a Click **Process the pending request and install the certificate**, and then click **Next**.



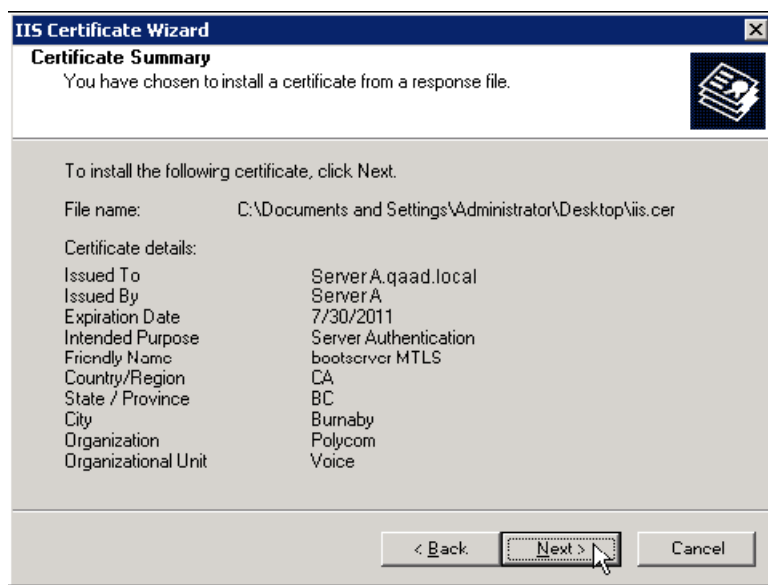
- b** Enter the location (for example, your desktop) of the IIS server certificate you created in the previous section [Creating the IIS Server Self-Signed Certificate for the IIS HTTPS Server](#), and then click **Next**.



- c** In the **SSL port this web site should use** box, enter **443**, and then click **Next**.



- d** Confirm the details of the certificate you are installing. Make sure the information next to **Issued To** is the fully qualified domain name of the IIS HTTPS virtual server.



The IIS server certificate is now installed on the IIS HTTPS virtual server.

Installing the Root CA Server Certificate on the Polycom Phone

After you create the root CA certificate during the procedure [Creating the IIS Server Self-Signed Certificate for the IIS HTTPS Server](#), install the certificate on the Polycom phone. If you used a certificate from a well-known certificate authority, install that certificate on the Polycom phone.



Note: Using the Touchscreen on the VVX 1500, VVX 500, and VVX 600

If you are installing the certificate on the VVX 1500, VVX 500, or VVX 600 phone, use the phone's touchscreen to navigate the installation.

To install the root CA server certificate on the Polycom phone:

- 1 Copy the root CA certificate to your boot server directory. You saved the certificate to your desktop in the previous section: [Creating the IIS Server Self-Signed Certificate for the IIS HTTPS Server](#).
- 2 On the Polycom phone, press the **Menu** button, and then select **Settings > Advanced**.
- 3 In the Password window, enter your password, and then press or tap **Enter**.
- 4 Do one of the following:

- If you have a SoundPoint IP or SoundStation IP phone, select **Admin Settings > Network Configuration > Server Menu**.
 - If you have a VVX 1500, VVX 500, or VVX 600 phone, select **Administration Settings > Network Configuration > Provisioning Server**.
- 5** In the Server Menu or Provisioning Server window, do the following:
- a** For **Server Type**, select **HTTP** (so that you can download the root CA certificate from your boot server), and then press or tap **OK**.
 - b** For **Server Address**, enter the server address of your HTTP boot server, and then press or tap **OK**.
 - c** For **Server User**, enter the user name to your HTTP boot server, and then press or tap **OK**.
 - d** For **Server Password**, enter the password to your HTTP boot server, and then press or tap **OK**.
- 6** Do one of the following:
- If you have a SoundPoint IP or SoundStation IP phone, press the **Back** soft key twice, and then save the new configuration.
 - If you have a VVX 1500, VVX 500, or VVX 600 phone, tap **Back** twice, and then save the new configuration.
- 7** Press the **Menu** button, and then select **Settings > Advanced**.
- 8** In the Password window, enter your password, and then press or tap **Enter**.
- 9** Do one of the following:
- If you have a SoundPoint IP or SoundStation IP phone, select **Admin Settings > SSL Security > CA Certificates > Install Custom CA Cert**.
 - If you have a VVX 1500, VVX 500, or VVX 600 phone, select **Administration Settings > TSL Security > Custom CA Certificates > Install Custom CA Cert**.
- 10** In the Install Custom CA Certificate window, enter the certificate file name or the location of the certificate for your root CA server, and then press or tap **Enter**.
- The phone will download the certificate and display the MD5 fingerprint.
- 11** To accept the certificate, press or tap **Accept**.
- 12** Do one of the following:
- If you have a SoundPoint IP or SoundStation IP phone, press the **Back** soft key, and then select **Configure CA Certs**.

- If you have a VVX 1500, VVX 500, or VVX 600 phone, tap **Back**, and then select **Configure CA Certificates**.

13 In the Configure CA Certificates window, select the **All Certificates** check box. This ensures that the custom certificate (the root CA certificate you loaded), as well as the default certificates, are active.



Note: Successful Downloading of Root CA Certificate

After you successfully download the root CA certificate for your server, the Polycom phone will trust your IIS HTTPS server.

14 Press the **Menu** button, and then select **Settings > Advanced**.

15 In the Password window, enter your password, and then press or tap **Enter**.

16 Do one of the following:

- If you have a SoundPoint IP or SoundStation IP phone, select **Admin Settings > Network Configuration > Server Menu**.
- If you have a VVX 1500, VVX 500, or VVX 600 phone, select **Administration Settings > Network Configuration > Provisioning Server**.

17 In the Server Menu or Provisioning Server window, for the **Server Type**, select **HTTPS**, and then press or tap **OK**.

18 Do one of the following:

- If you have a SoundPoint IP or SoundStation IP phone, press the **Back** soft key twice, and then save the new configuration.
- If you have a VVX 1500, VVX 500, or VVX 600 phone, tap **Back** twice, and then save the new configuration.

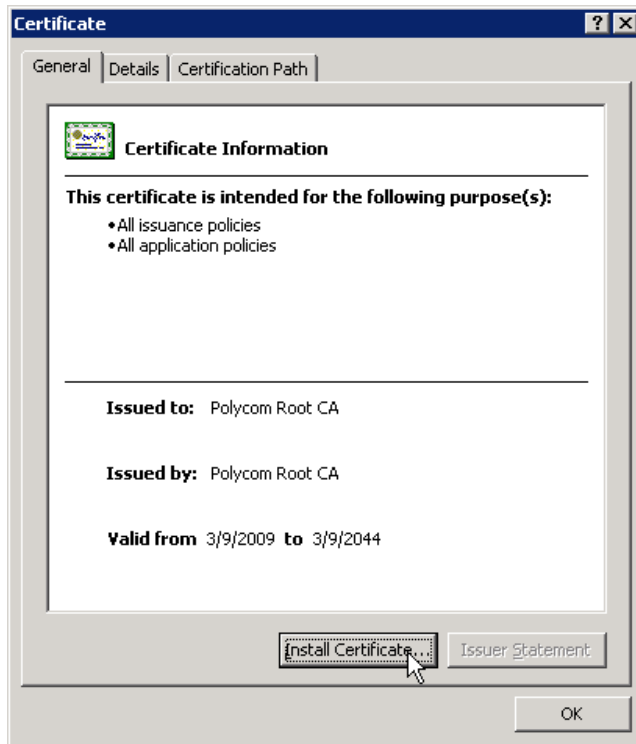
Installing the Polycom Root CA Certificate on the Microsoft Certificate Authority Server

Skip this section if you are using a certificate from a well-known certificate authority. If you plan to run your own certificate authority, complete the steps in this section.

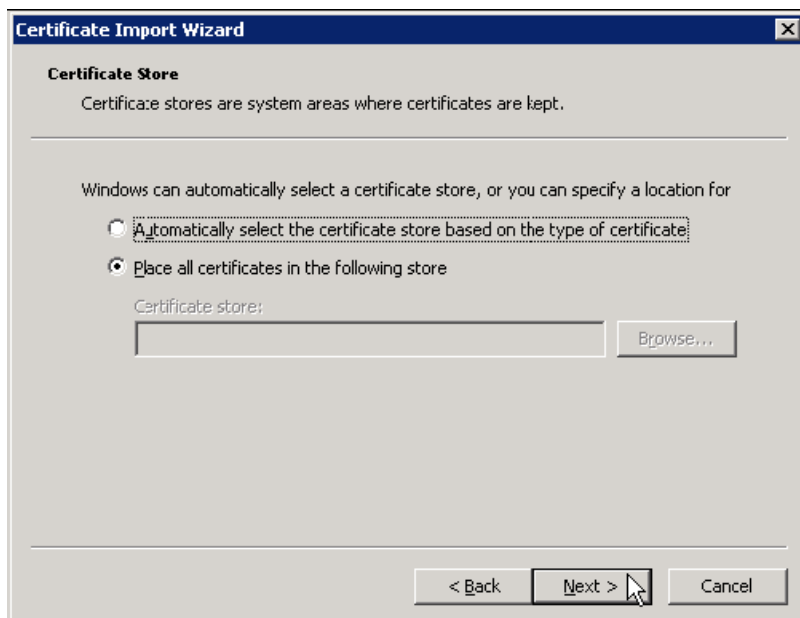
To install the Polycom root CA certificate on the Microsoft Certificate Authority Server:

- 1** Access the [Polycom Root CA Certificate](#).

- 2 The certificate will display. Click **Install Certificate**.



- 3 From the Certificate Import Wizard, do the following:
 - a Click **Place all certificates in the following store**, and then click **Next**.



- b From the Select Certificate Store window, double-click **Trusted Root Certification Authorities**, and then click **Local Computer**. Then, select the **Show Physical Stores** check box, and then press **OK**.



Note: Selecting the Local Computer Certificate Store

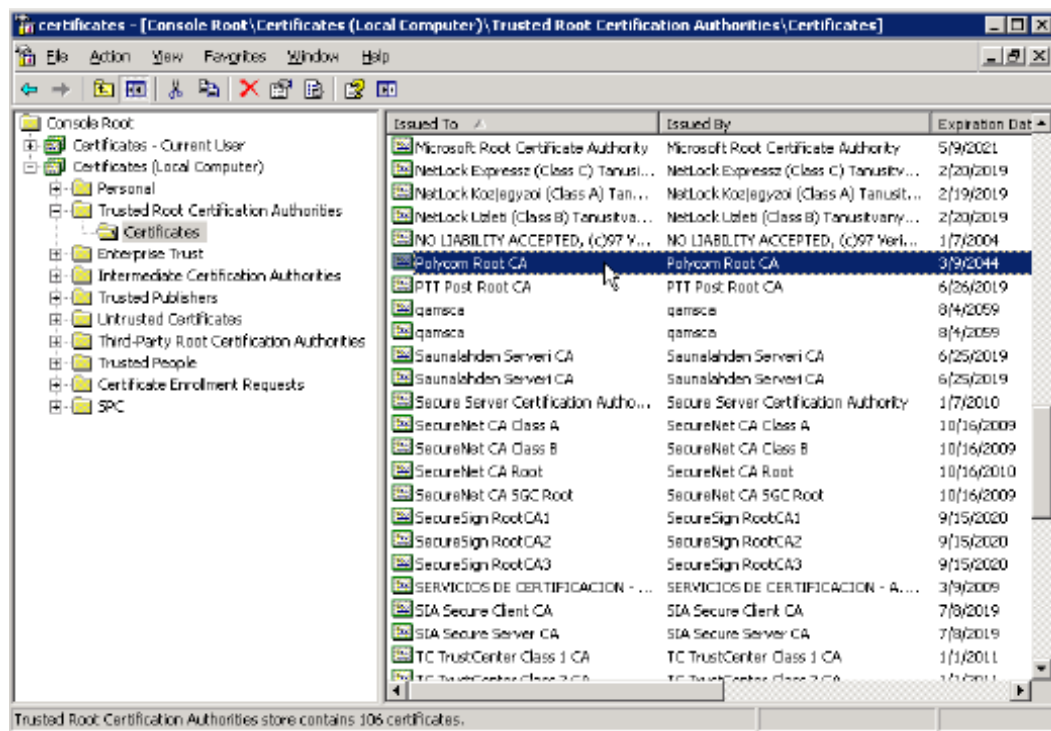
If you do not select the local computer certificate store, the server will not recognize any Polycom client certificates.

c Click Finish.



The Polycom Root CA certificate is now installed on your server.

To verify that the certificate is installed correctly, open the Certificates module in Microsoft Management Console (MMC) and confirm that the Polycom Root CA is listed.





Note: Installing Intermediate Certificates

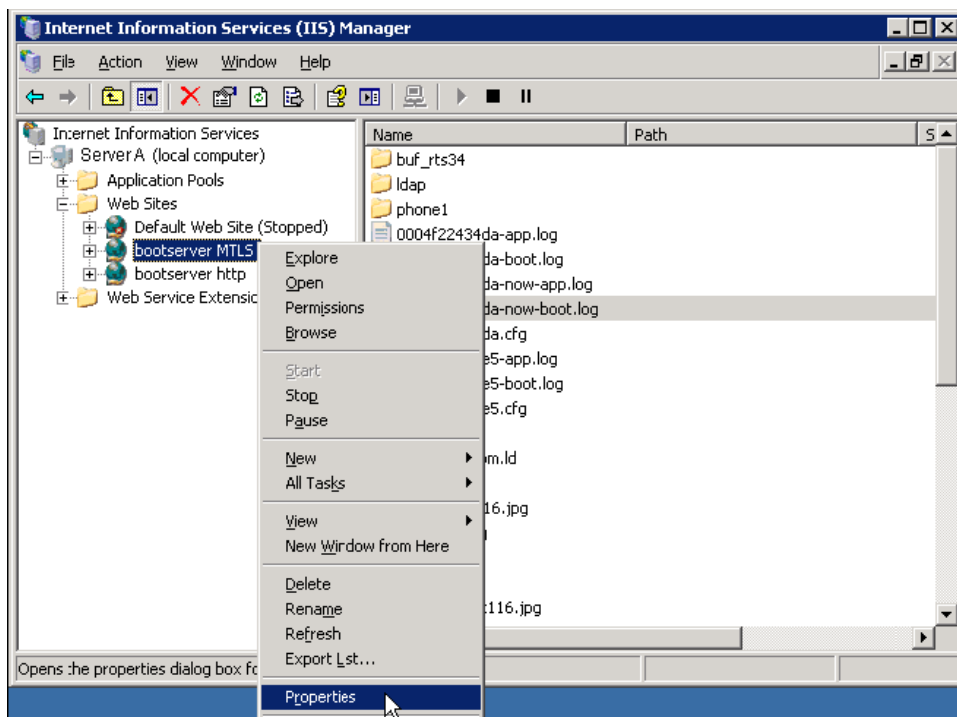
If your root CA does not recognize the Polycom intermediate CAs, you may have to install the intermediate certificates, or configure Microsoft to automatically download the intermediate certificates. For more information, see [Troubleshooting](#).

Enabling Mutual TLS on the IIS Server

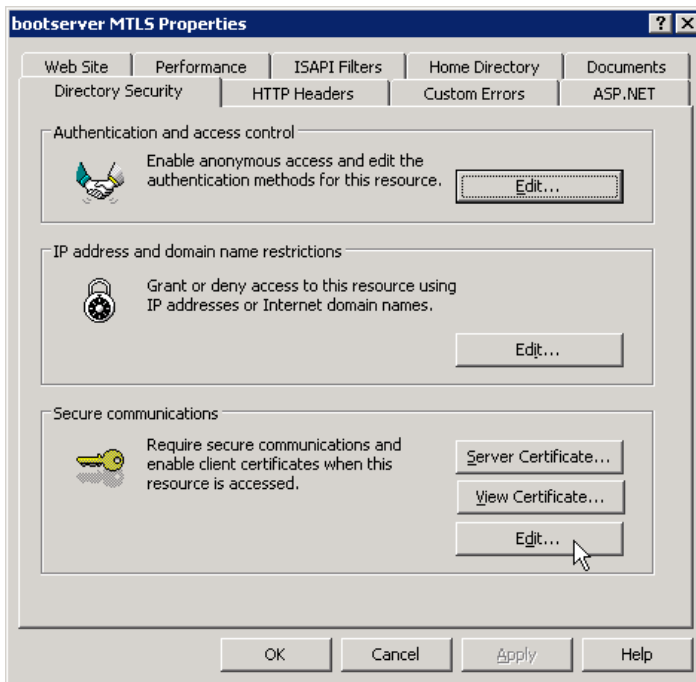
To enable mutual TLS on the IIS server, you must set the IIS server to require a Client Certificate.

To enable mutual TLS on the IIS server:

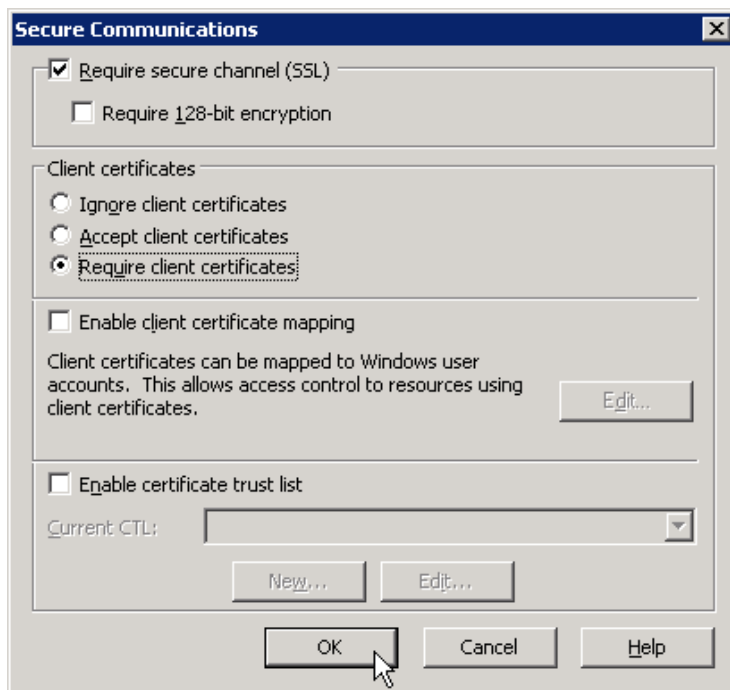
- 1 Open Internet Information Services (IIS) Manager. Right-click the HTTPS virtual server (for example, **bootserver MTLs**), and then select **Properties**.



- 2 From the Properties window, click the **Directory Security** tab. In the **Secure communications** area, click **Edit**.



- 3 From the Secure Communications window, select the **Require secure channel (SSL)** check box, and in the **Client certificates** area, click **Require client certificates**. Click **OK**.



- 4 At the server command prompt, type **IISRESET** to reset the IIS Server.
- 5 Reboot the phone.
The bootROM will now use HTTP with digest authentication, and the application will use mutual TLS.

Troubleshooting

If you have problems with the configuration, Polycom recommends consulting the troubleshooting tips in this section before contacting Polycom Support.

How Can I Tell if Mutual TLS is Working?

In the serial log, you will see `<MACaddress>.cfg` being downloaded.

The first section of the log shows one-way SSL working correctly:

```
0727210309|copy |3|00|'https://:****@Server A.qaad.local/0004f22434da.cfg'  
from 'Server A.qaad.local(172.23.0.81)'  
0727210309|curl |3|00|timeout on name lookup is not supported  
0727210309|curl |3|00|About to connect() to Server A.qaad.local port 443  
(#0)  
0727210309|curl |3|00| Trying 172.23.0.81...  
0727210309|curl |3|00|Connected to Server A.qaad.local (172.23.0.81) port  
443 (#0)  
0727210309|curl |3|00|successfully set certificate verify locations:  
0727210309|curl |3|00| CAfile: /ffs0/ca-bundle.crt CApath: none  
0727210309|curl |3|00|SSLv3, TLS handshake, Client hello (1):  
0727210309|curl |3|00|SSLv3, TLS handshake, Server hello (2):  
0727210309|curl |3|00|SSLv3, TLS handshake, CERT (11):  
0727210309|curl |3|00|SSLv3, TLS handshake, Server finished (14):  
0727210309|curl |3|00|SSLv3, TLS handshake, Client key exchange (16):  
0727210309|curl |3|00|SSLv3, TLS change cipher, Client hello (1):  
0727210309|curl |3|00|SSLv3, TLS handshake, Finished (20):  
0727210309|curl |3|00|SSLv3, TLS change cipher, Client hello (1):  
0727210309|curl |3|00|SSLv3, TLS handshake, Finished (20):  
0727210309|curl |3|00|SSL connection using RC4-SHA  
0727210309|curl |3|00|Server certificate:  
0727210309|curl |3|00|  subject: C=CA, ST=burnaby, L=bc, O=polycom,  
OU=polycom, CN=Server A.qaad.local  
0727210309|curl |3|00|  start date: 2009-07-23 21:04:34 GMT  
0727210309|curl |3|00|  expire date: 2011-07-23 21:04:34 GMT  
0727210309|curl |3|00|  common name: Server A.qaad.local (matched)  
0727210309|curl |3|00|  issuer: DC=local, DC=qaad, CN=Server A  
0727210309|curl |3|00|  SSL certificate verify ok.
```

The second section of the log shows mutual TLS being established:

```
0727210309|curl |3|00|SSLv3, TLS handshake, Hello request (0):
0727210309|curl |3|00|SSLv3, TLS handshake, Client hello (1):
0727210309|curl |3|00|SSLv3, TLS handshake, Server hello (2):
0727210309|curl |3|00|SSLv3, TLS handshake, CERT (11):
0727210309|curl |3|00|SSLv3, TLS handshake, Request CERT (13):
0727210309|curl |3|00|SSLv3, TLS handshake, Server finished (14):
0727210309|curl |3|00|SSLv3, TLS handshake, CERT (11):
0727210309|curl |3|00|SSLv3, TLS handshake, Client key exchange (16):
0727210309|curl |3|00|SSLv3, TLS handshake, CERT verify (15):
0727210309|curl |3|00|SSLv3, TLS change cipher, Client hello (1):
0727210309|curl |3|00|SSLv3, TLS handshake, Finished (20):
0727210309|curl |3|00|SSLv3, TLS change cipher, Client hello (1):
0727210309|curl |3|00|SSLv3, TLS handshake, Finished (20):
0727210309|curl |3|00|Connection #0 to host Server A.qaad.local left intact
```

These SSL logs are created for each file that is accessed.

You can verify that mutual TLS is working correctly when `<MACaddress>.cfg` is downloaded successfully:

```
0727210309|copy |3|00|Download of '0004f22434da.cfg' succeeded on attempt 1
(addr 1 of 1)
```

Mutual TLS is not working correctly if you receive a 403 error. You may also receive 404 errors that indicate that files cannot be found on your boot server.

How Can I Verify a Custom Certificate is Installed on the Phone?

For authorized Polycom technicians that have access to the serial console, type `copy ca-bundle.crt` at the serial prompt. The default certificates will be displayed and the last entry will be the custom certificate. You can view the certificate and compare it to the one on the server.

How Can I Erase the Certificates I've Installed on the Phone?

You can perform a MAC Reset on the phone, which will reset your phone to factory defaults. You can also overwrite a previously installed custom certificate by loading a new custom certificate.

Windows Server 2003 and Windows XP Clients Cannot Obtain Certificates from a Windows Server 2008-Based CA

Windows Server 2003 and Windows XP clients cannot obtain certificates from a Windows Server 2008-based CA if the CA is configured to use SHA2 256 or higher encryption. To obtain the required patch, go to [Microsoft Support 968730](#).

Intermediate Certificates Are Not Downloaded to Complete a Certificate Chain by Default

Go to [Security-Related Changes in Authentication \(IIS 6.0\)](#) and see the topic “Intermediate Certificates Are Not Downloaded to Complete a Certificate Chain”. For information about manually updating the certificate store, select “Client receives 403.16 error when IIS cannot process a complete certificate chain” on the same web page.

For more information, see the article [Http.sys registry settings for Windows](#).

Additional Information

For more information on HTTP and HTTPS provisioning, including Digest authentication, see the following:

- [Polycom UC Software 4.1.0 Administrators' Guide](#)
- [Digest authentication and Advanced Digest authentication in Windows Server 2003](#)

Trademarks

©2013, Polycom, Inc. All rights reserved.

POLYCOM®, the Polycom logo and the names and marks associated with Polycom products are trademarks and/or service marks of Polycom, Inc. and are registered and/or common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Polycom.

Disclaimer

While Polycom uses reasonable efforts to include accurate and up-to-date information in this document, Polycom makes no warranties or representations as to its accuracy. Polycom assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

Limitation of Liability

Polycom and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall Polycom and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if Polycom has been advised of the possibility of such damages.

Customer Feedback

We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocumentationFeedback@polycom.com.



Visit support.polycom.com for software downloads, product documents, product licenses, troubleshooting tips, service requests, and more.