Technical Bulletin 52609

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

This technical bulletin 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).

The information in this bulletin applies to IIS 6.0 on Windows Server® 2003, and SoundPoint IP, SoundStation IP, and VVX phones running SIP application version 3.2 or later.

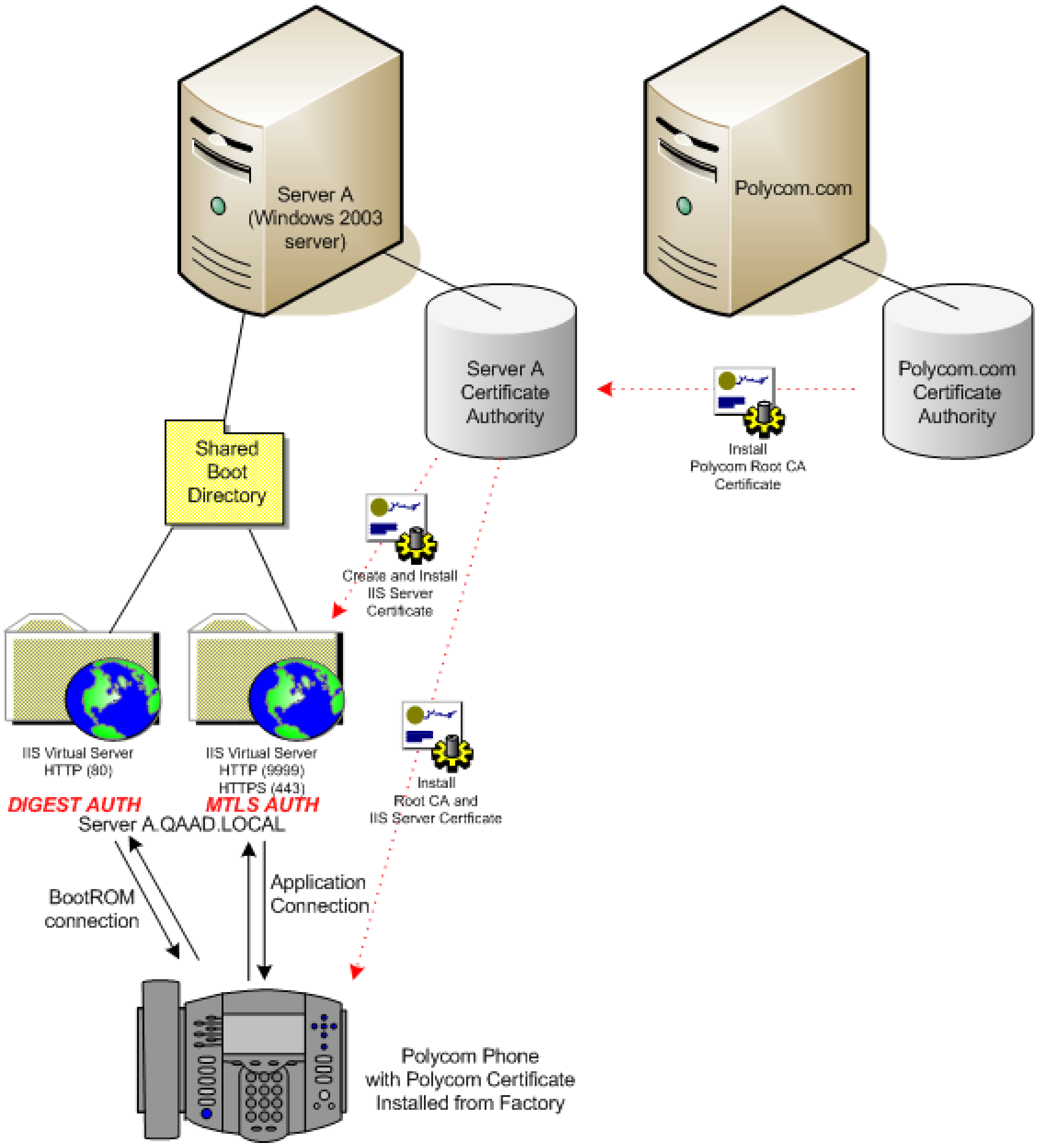
The topics include:

- Overview, below.
- Mutual TLS Requirements on page 3.
- Configuring Mutual TLS Provisioning on page 3.
- Troubleshooting on page 45.
- Additional Information on page 46.

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.

Note 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

- 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, available at http://pki.polycom.com/pki/Polycom%20Root%20CA.crt.
- Patch for Microsoft server to use SHA2 256 or higher encryption. For more information, see the related entry in the Troubleshooting section on page 45.

Configuring Mutual TLS Provisioning

Configuring mutual TLS provisioning involves the following steps:

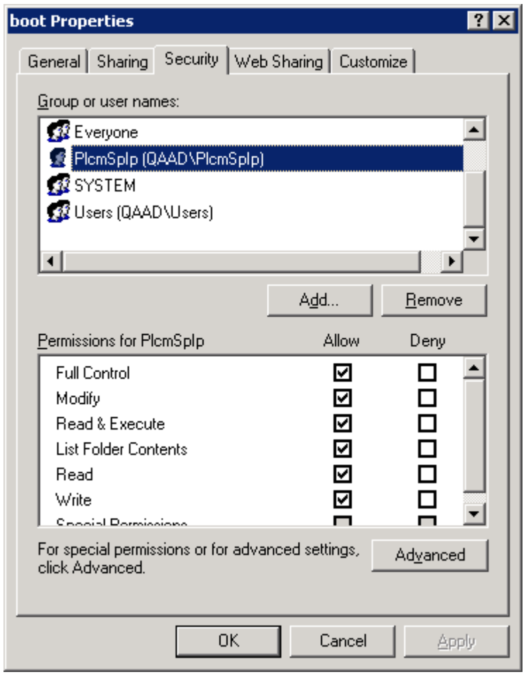
1. Creating a Directory on the IIS Server on page 4.
2. Creating the HTTP Virtual Server in IIS on page 5.
3. Creating the HTTPS Virtual Server in IIS on page 12.
4. Installing Microsoft Certificate Service on page 18.
5. Creating the IIS Server Self-Signed Certificate for the IIS HTTPS Server on page 21.
6. Installing the Server Certificate on the IIS Server on page 33.
7. Installing the Root CA Server Certificate on the Polycom Phone on page 36.
8. Installing the Polycom Root CA Certificate on the Microsoft Certificate Authority Server on page 38.
9. Enabling Mutual TLS on the IIS Server on page 42.

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.



Group or user names:

- Everyone
- PlcmSplp (QAAD\PlcmSplp)
- SYSTEM
- Users (QAAD\Users)

Permissions for PlcmSplp	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□
Special Permissions	□	□

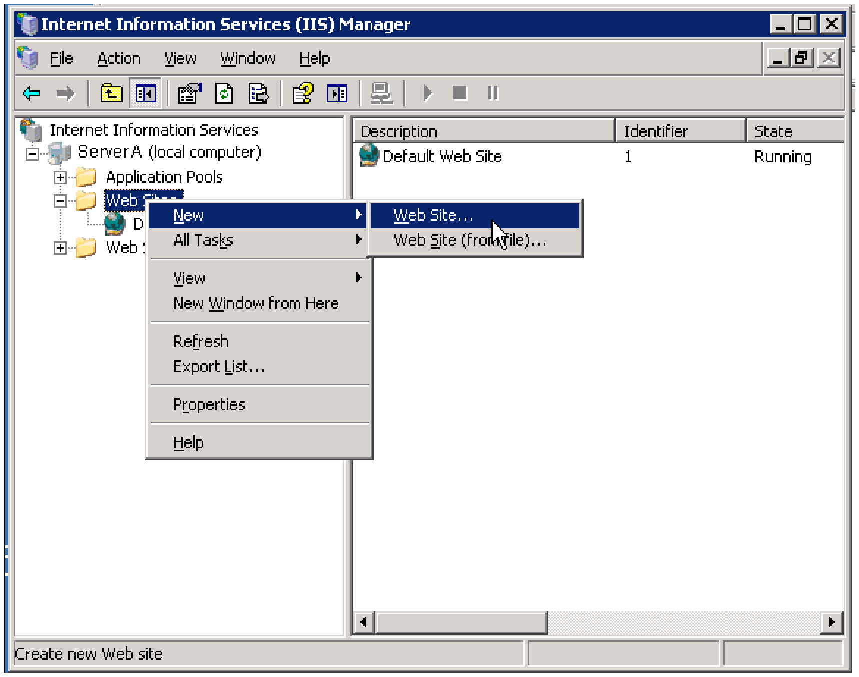
For special permissions or for advanced settings, click Advanced.

Creating the HTTP Virtual Server in IIS

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

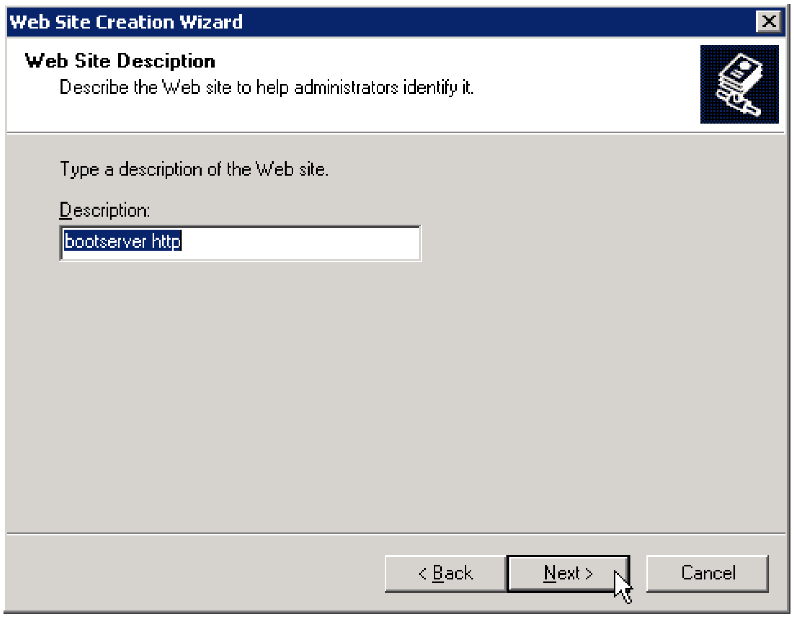
To create the HTTP virtual server:

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:

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

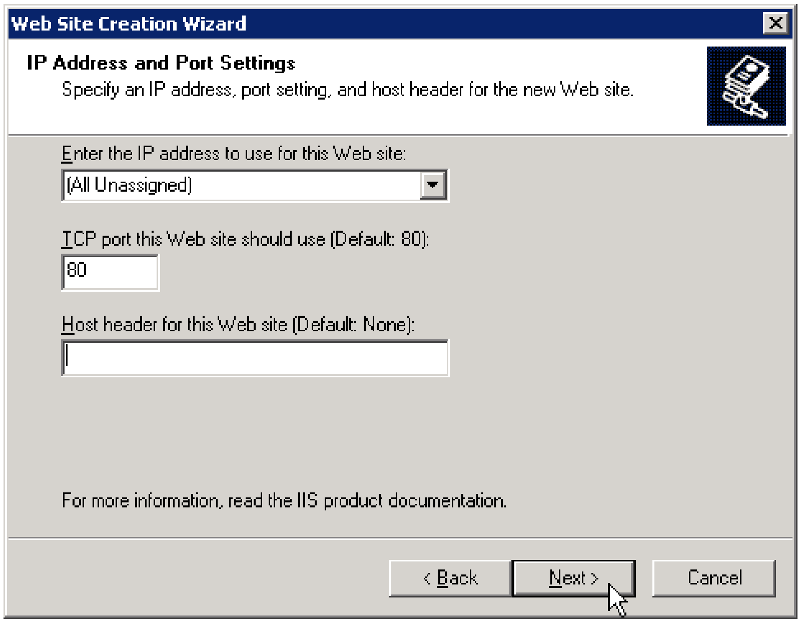


Web Site Description
Describe the Web site to help administrators identify it.

Type a description of the Web site.

Description: bootserver http

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



IP Address and Port Settings
Specify an IP address, port setting, and host header for the new Web site.

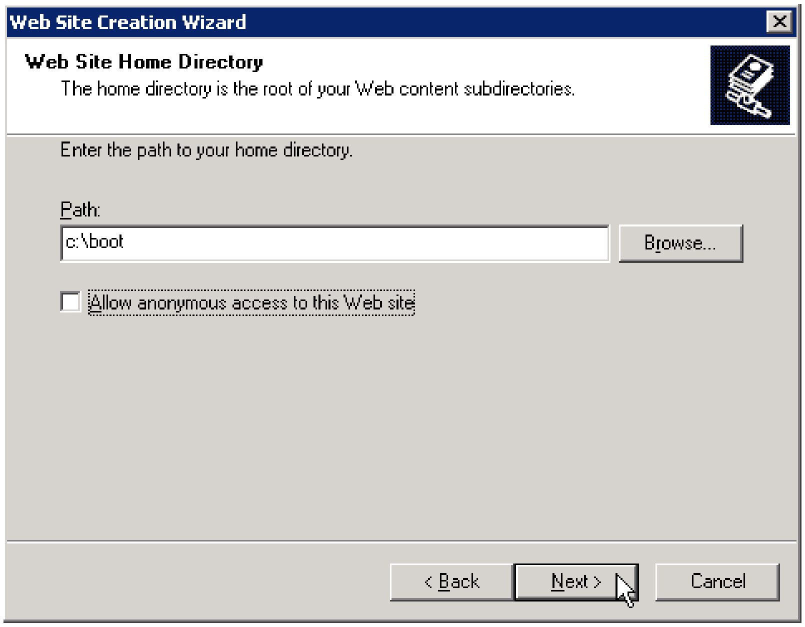
Enter the IP address to use for this Web site: (All Unassigned)

TCP port this Web site should use (Default: 80): 80

Host header for this Web site (Default: None):

For more information, read the IIS product documentation.

- 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**.



Web Site Creation Wizard

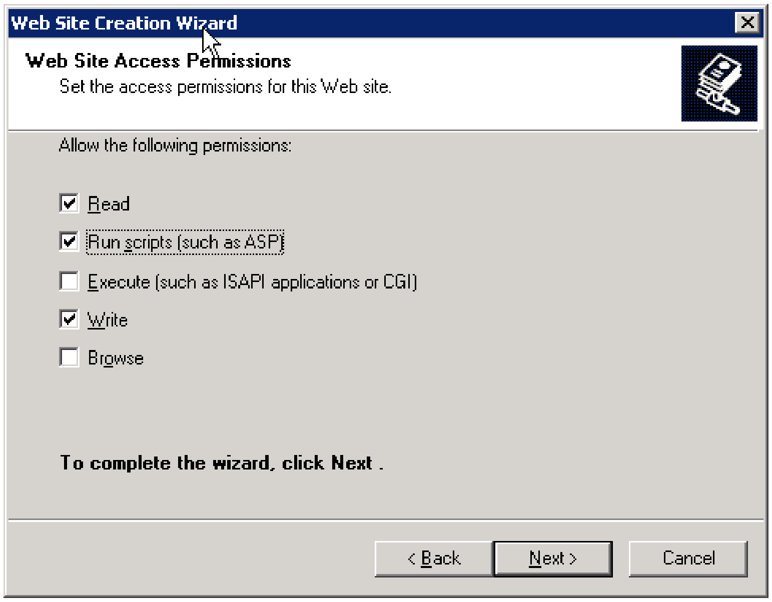
Web Site Home Directory
The home directory is the root of your Web content subdirectories.

Enter the path to your home directory.

Path:
c:\boot

☐ Allow anonymous access to this Web site

- 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.)



Web Site Creation Wizard

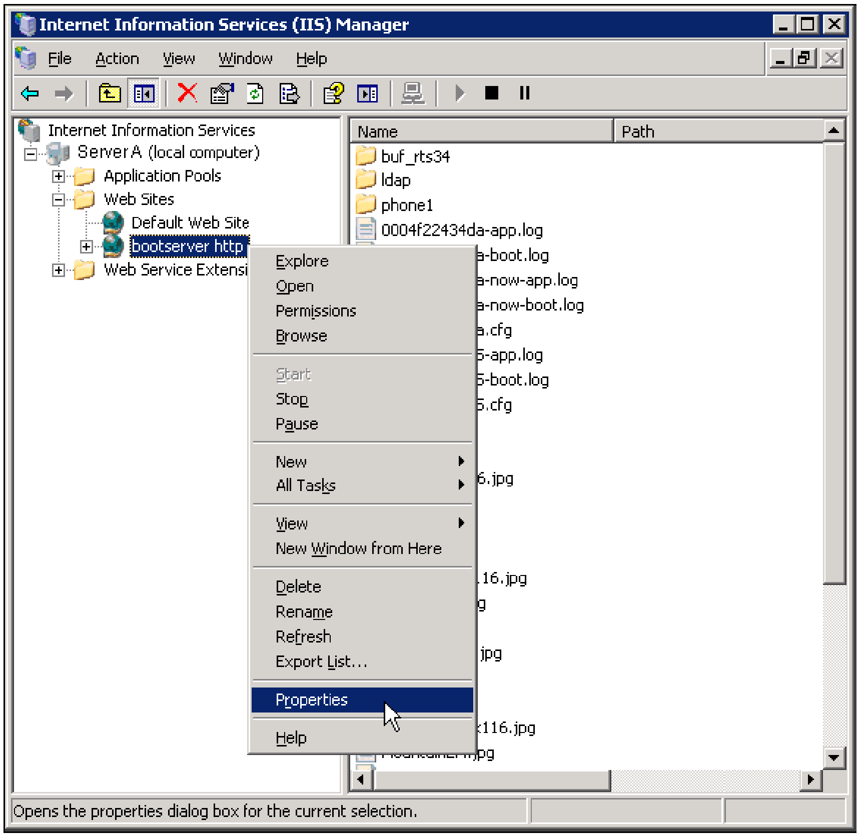
Web Site Access Permissions
Set the access permissions for this Web site.

Allow the following permissions:

☑ Read
☑ Run scripts (such as ASP)
☐ Execute (such as ISAPI applications or CGI)
☑ Write
☐ Browse

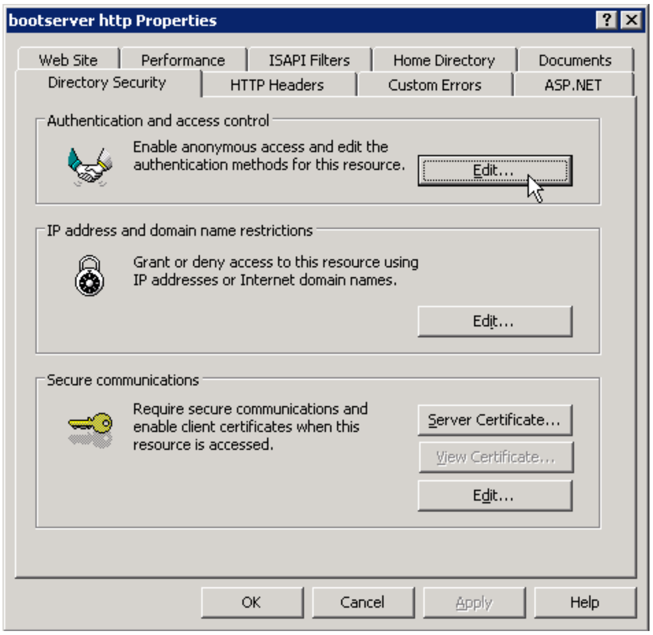
To complete the wizard, click Next .

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



Opens the properties dialog box for the current selection.

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

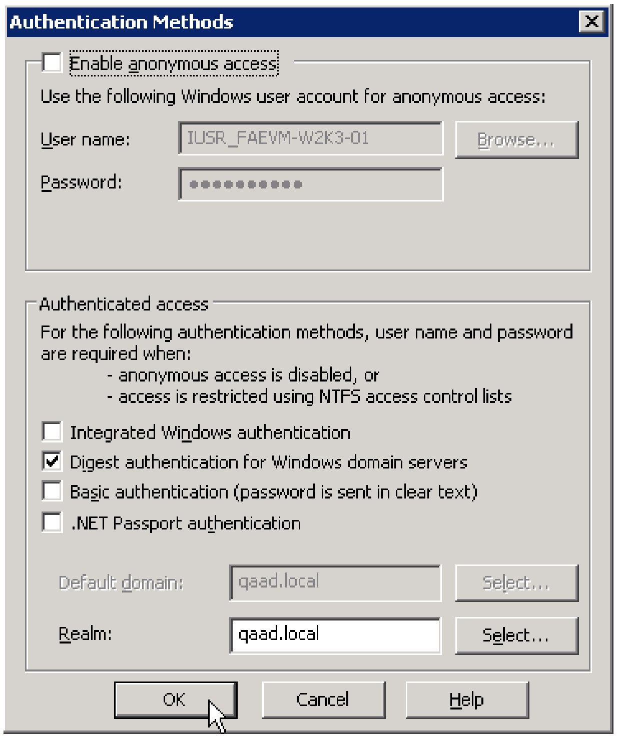


Enable anonymous access and edit the authentication methods for this resource.

Grant or deny access to this resource using IP addresses or Internet domain names.

Require secure communications and enable client certificates when this resource is accessed.

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.)



Authentication Methods

□ Enable anonymous access

Use the following Windows user account for anonymous access:

User name: IUSR_FAEVM-W2K3-01

Password: ●●●●●●●●●●

Authenticated access

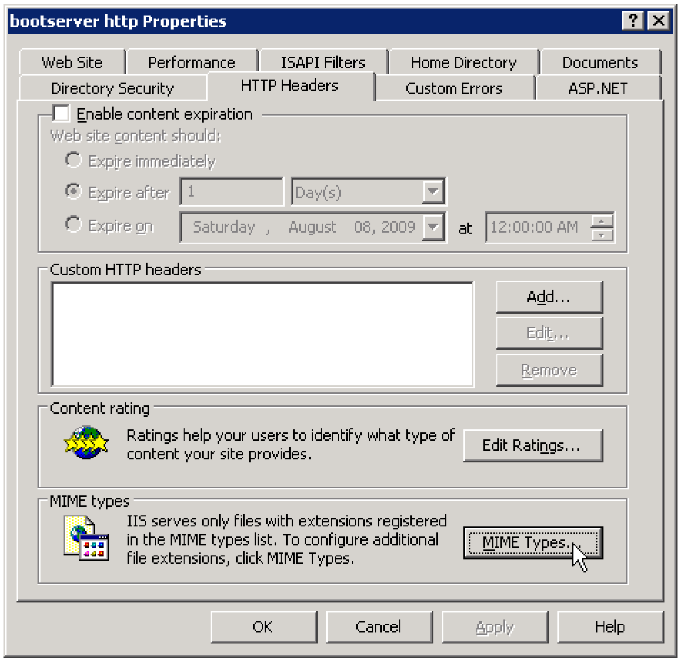
For the following authentication methods, user name and password are required when:
- anonymous access is disabled, or
- access is restricted using NTFS access control lists

□ Integrated Windows authentication
☑ Digest authentication for Windows domain servers
□ Basic authentication (password is sent in clear text)
□ .NET Passport authentication

Default domain: qaad.local

Realm: qaad.local

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



☐ Enable content expiration

Web site content should:

○ Expire immediately

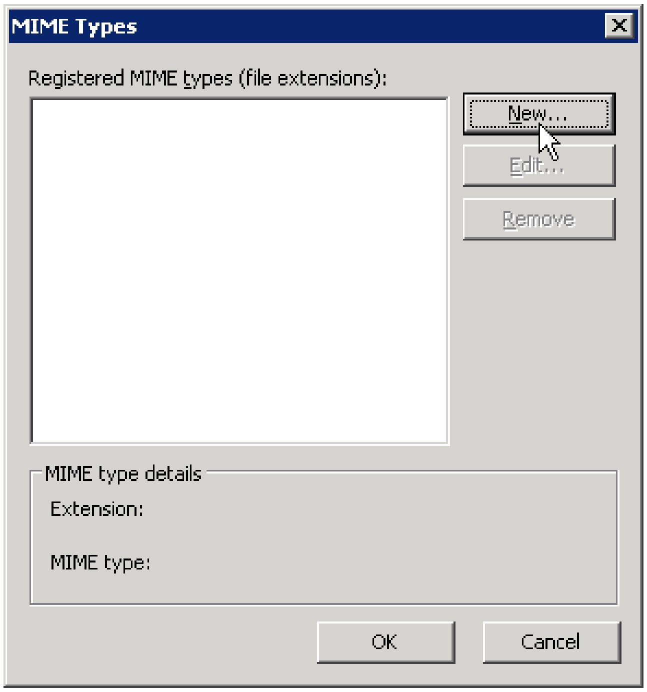
● Expire after 1 Day(s)

○ Expire on Saturday , August 08, 2009 at 12:00:00 AM

Ratings help your users to identify what type of content your site provides.

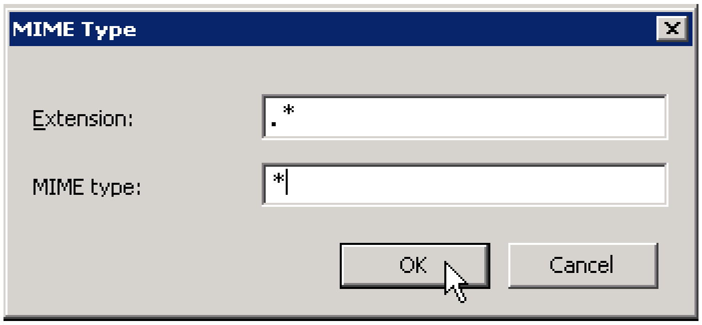
IIS serves only files with extensions registered in the MIME types list. To configure additional file extensions, click MIME Types.

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



8. From the MIME Type window, do the following:
   - In the **Extension** box, enter **.***
   - In the **MIME type** box, enter *
   - Click **OK**.

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



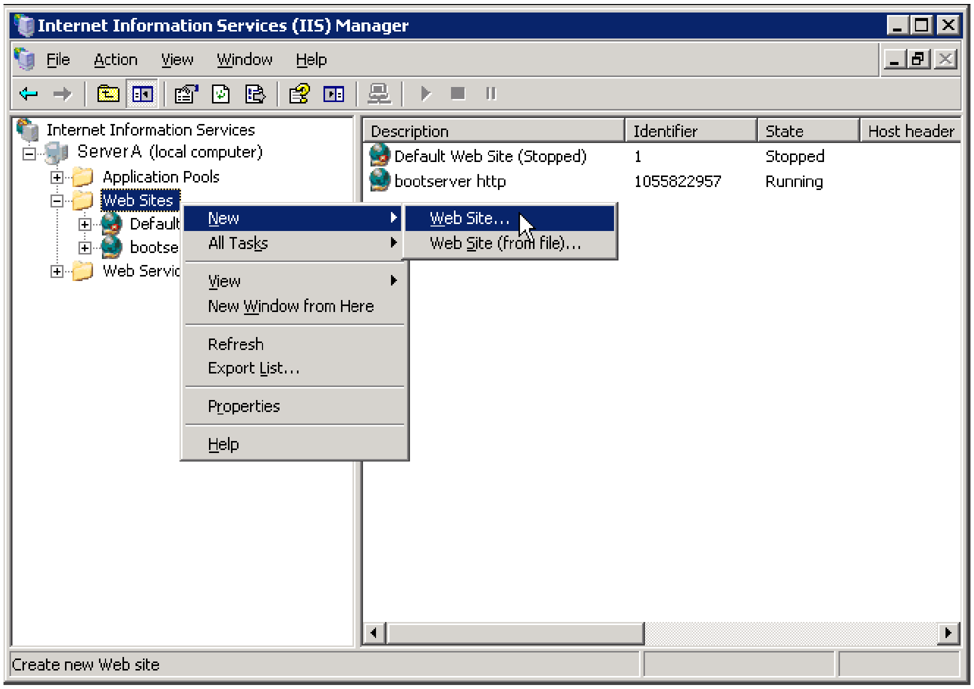
Extension: .*
MIME type: *

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:

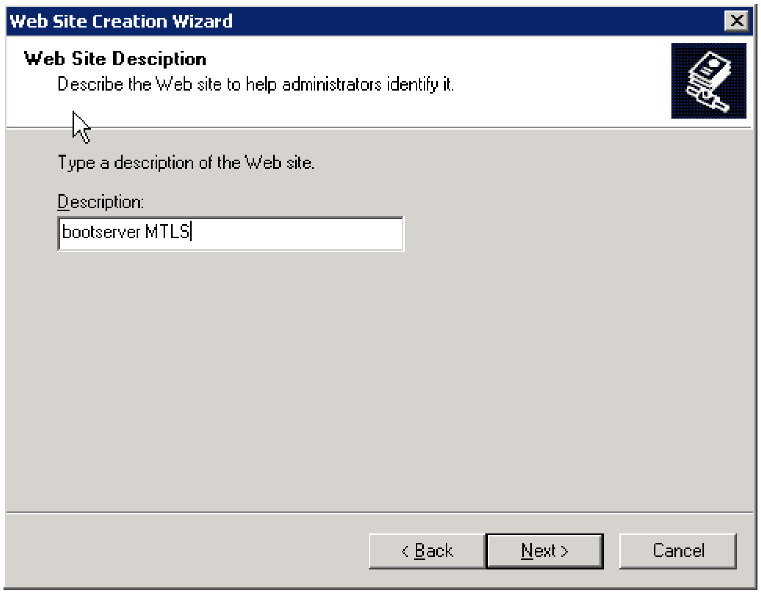
1. Open Internet Information Services (IIS) Manager. Right-click **Web Sites**, and then select **New** > **Web Site**.



Description	Identifier	State	Host header
Default Web Site (Stopped)	1	Stopped	
bootserver http	1055822957	Running	

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

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



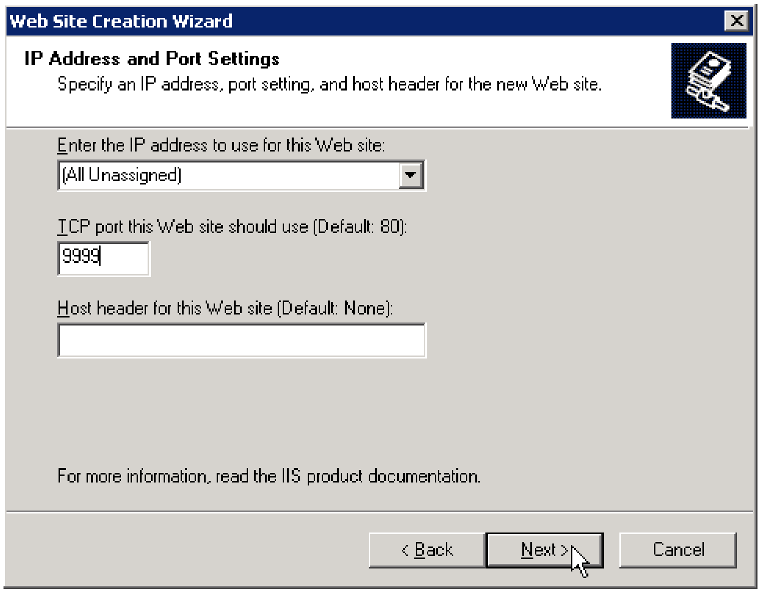
Web Site Description

Describe the Web site to help administrators identify it.

Type a description of the Web site.

Description: bootserver MTLS

— 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**.



Web Site Creation Wizard

IP Address and Port Settings

Specify an IP address, port setting, and host header for the new Web site.

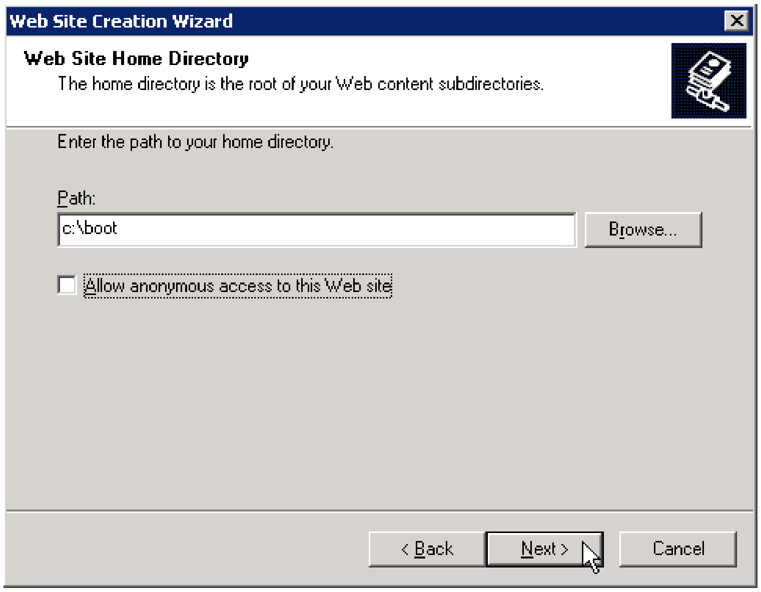
Enter the IP address to use for this Web site: (All Unassigned)

TCP port this Web site should use (Default: 80): 9999

Host header for this Web site (Default: None):

For more information, read the IIS product documentation.

— 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**.



Web Site Creation Wizard

Web Site Home Directory

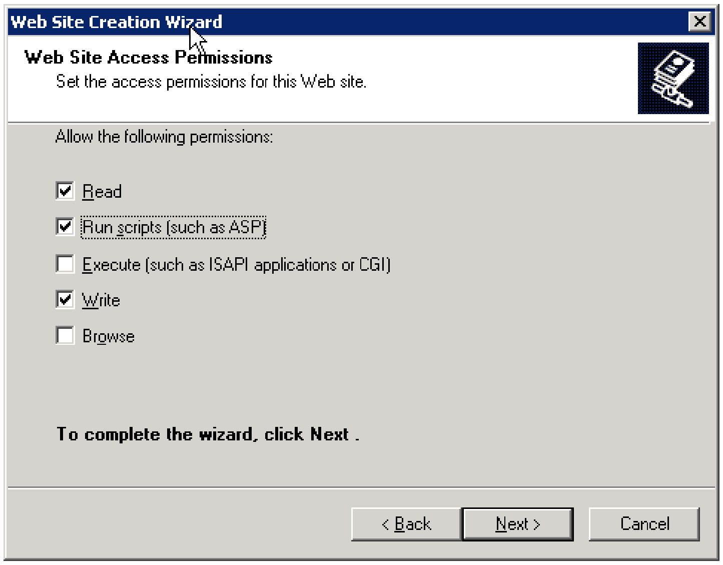
The home directory is the root of your Web content subdirectories.

Enter the path to your home directory.

Path: c:\boot

☐ Allow anonymous access to this Web site

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



Web Site Creation Wizard

Web Site Access Permissions

Set the access permissions for this Web site.

Allow the following permissions:

☑ Read

☑ Run scripts (such as ASP)

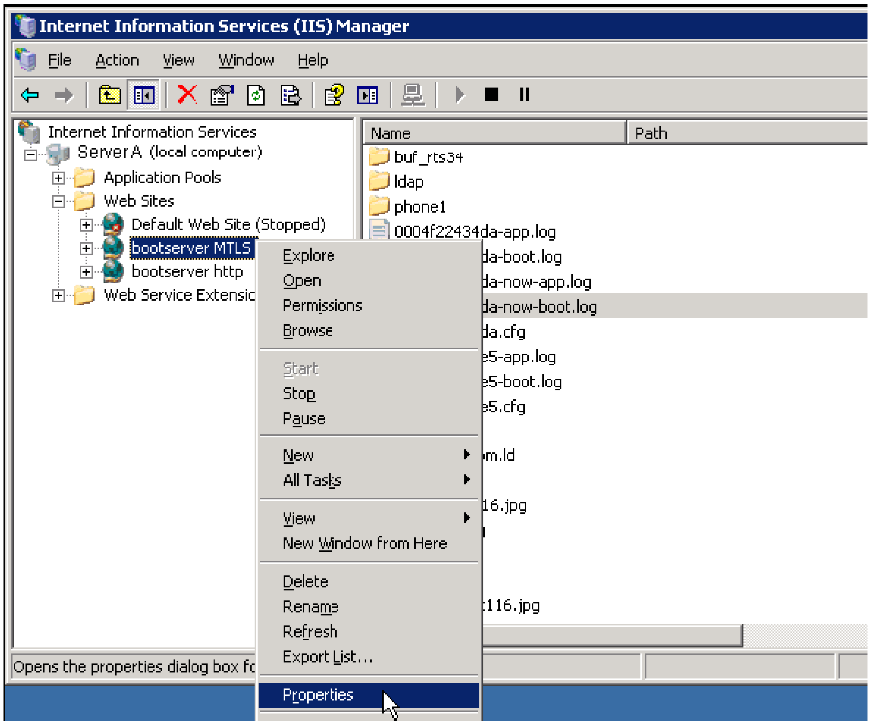
☐ Execute (such as ISAPI applications or CGI)

☑ Write

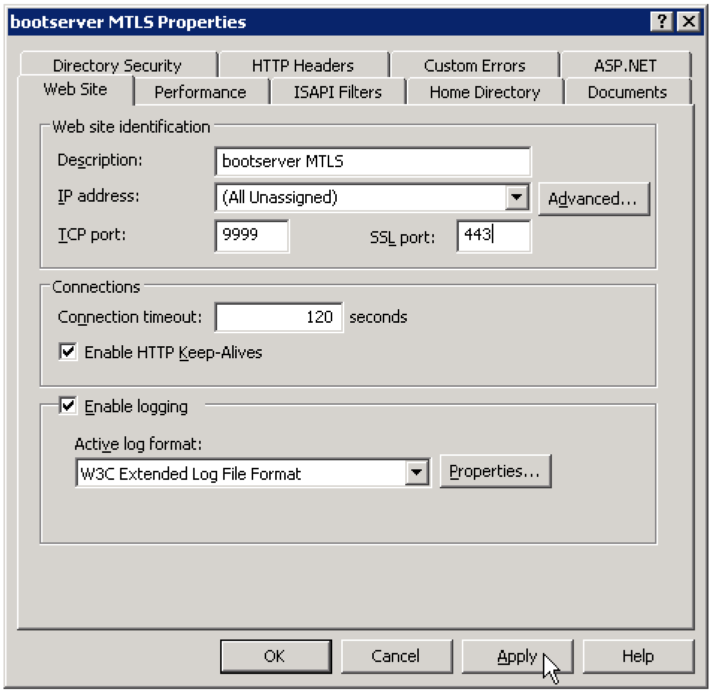
☐ Browse

To complete the wizard, click Next .

3. From the Internet Information Services (IIS) Manager window, right-click the virtual server (for example, **bootserver MTLS**), 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**.



Web site identification

Description: bootserver MTLS

IP address: (All Unassigned)

TCP port: 9999   SSL port: 443

Connections

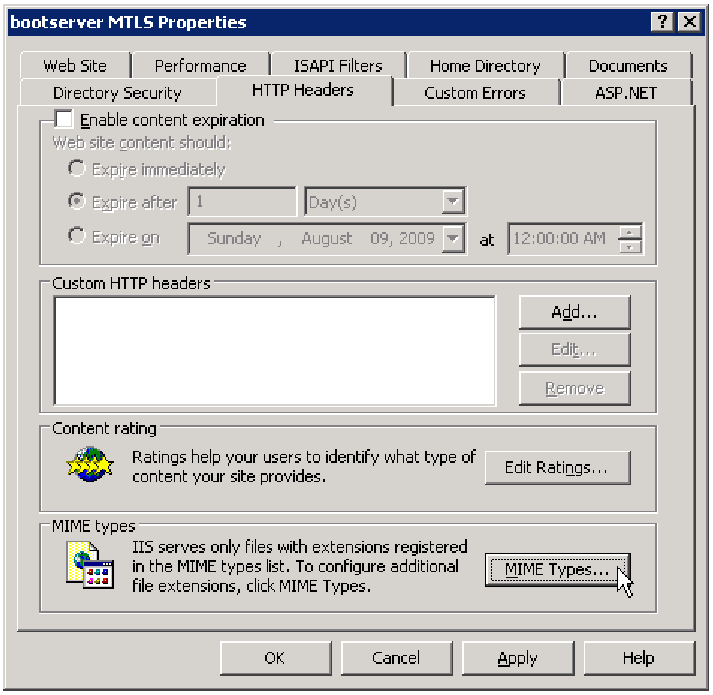
Connection timeout: 120 seconds

☑ Enable HTTP Keep-Alives

☑ Enable logging

Active log format: W3C Extended Log File Format

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



□ Enable content expiration

Web site content should:

○ Expire immediately

● Expire after 1 Day(s)

○ Expire on Sunday , August 09, 2009 at 12:00:00 AM

Custom HTTP headers

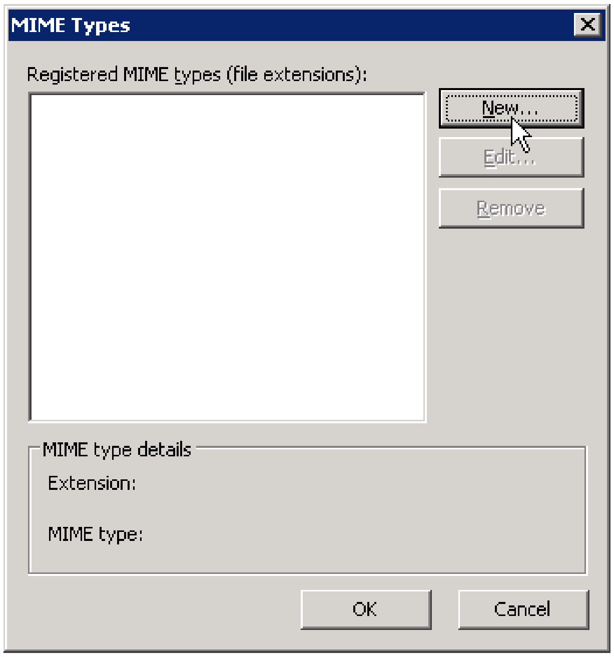
Content rating

Ratings help your users to identify what type of content your site provides.

MIME types

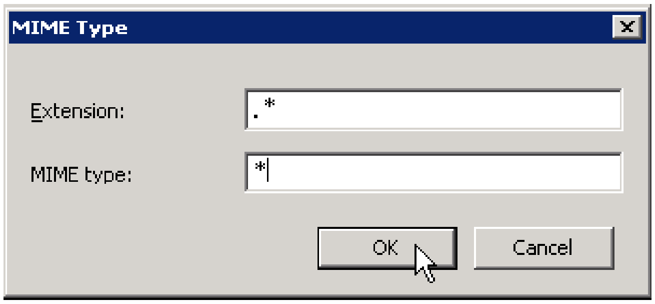
IIS serves only files with extensions registered in the MIME types list. To configure additional file extensions, click MIME Types.

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



7. From the MIME Type window, do the following:
   - In the **Extension** box, enter **.***
   - In the **MIME type** box, enter *****
   - Click **OK**.

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



Extension: .*

MIME type: *

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

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

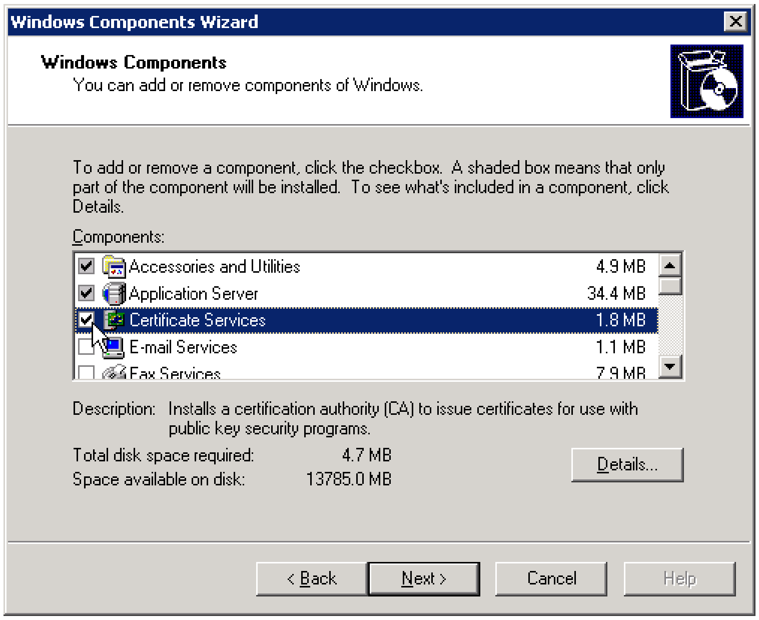
Installing Microsoft Certificate Service

Note 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 following steps.

Note Before you complete the following steps, 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, on the far-right of the screen, click **Add/Remove Windows Components.**
2. From the Windows Components Wizard window, do the following:
   – Select the **Certificate Services** check box, and then click **Next**.



Windows Components

You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

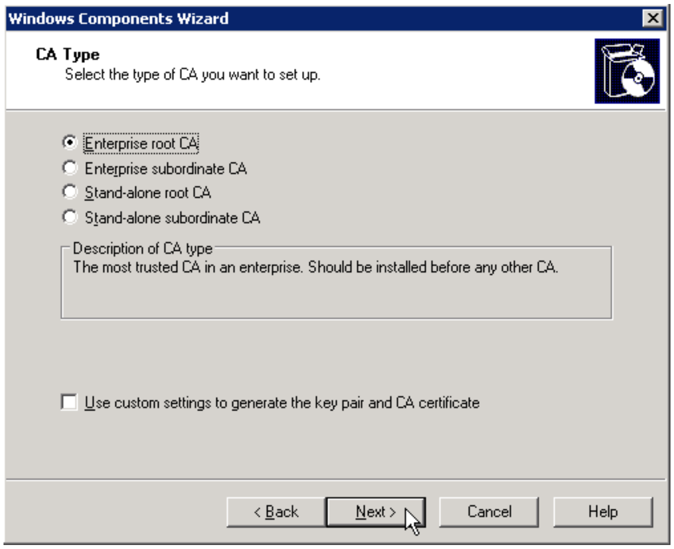
☑	Accessories and Utilities	4.9 MB
☑	Application Server	34.4 MB
☑	Certificate Services	1.8 MB
☐	E-mail Services	1.1 MB
☐	Fax Services	7.9 MB

Description: Installs a certification authority (CA) to issue certificates for use with public key security programs.

Total disk space required: 4.7 MB

Space available on disk: 13785.0 MB

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



Windows Components Wizard

CA Type

Select the type of CA you want to set up.

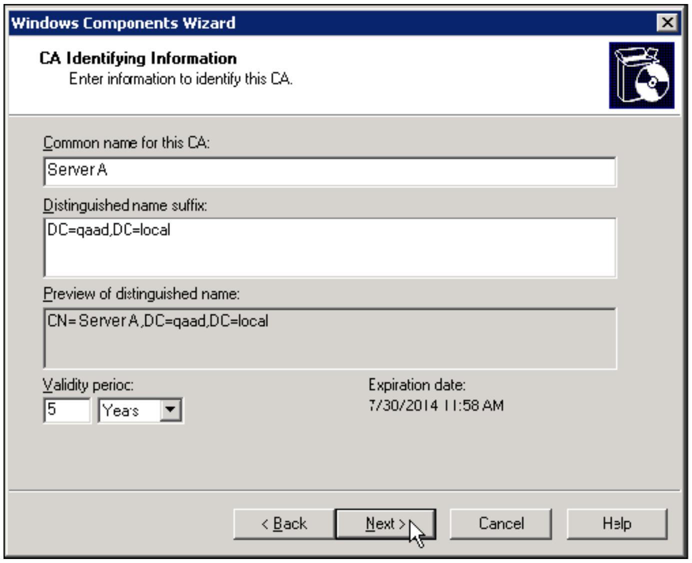
● Enterprise root CA
○ Enterprise subordinate CA
○ Stand-alone root CA
○ Stand-alone subordinate CA

Description of CA type

The most trusted CA in an enterprise. Should be installed before any other CA.

□ Use custom settings to generate the key pair and CA certificate

— 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**.



Windows Components Wizard

CA Identifying Information

Enter information to identify this CA.

Common name for this CA: Server A

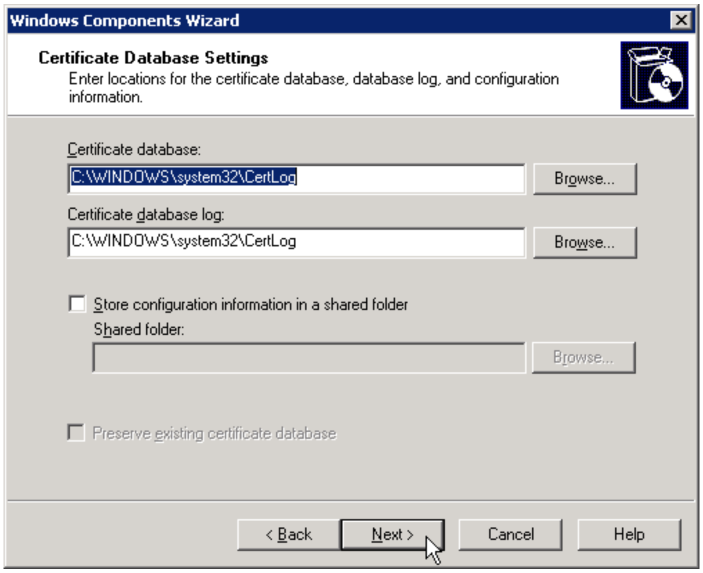
Distinguished name suffix: DC=qaad,DC=local

Preview of distinguished name: CN=Server A,DC=qaad,DC=local

Validity period: 5 Years

Expiration date: 7/30/2014 11:58 AM

- 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**.



Windows Components Wizard

Certificate Database Settings

Enter locations for the certificate database, database log, and configuration information.

Certificate database: C:\WINDOWS\system32\CertLog

Certificate database log: C:\WINDOWS\system32\CertLog

□ Store configuration information in a shared folder

Shared folder:

□ Preserve existing certificate database

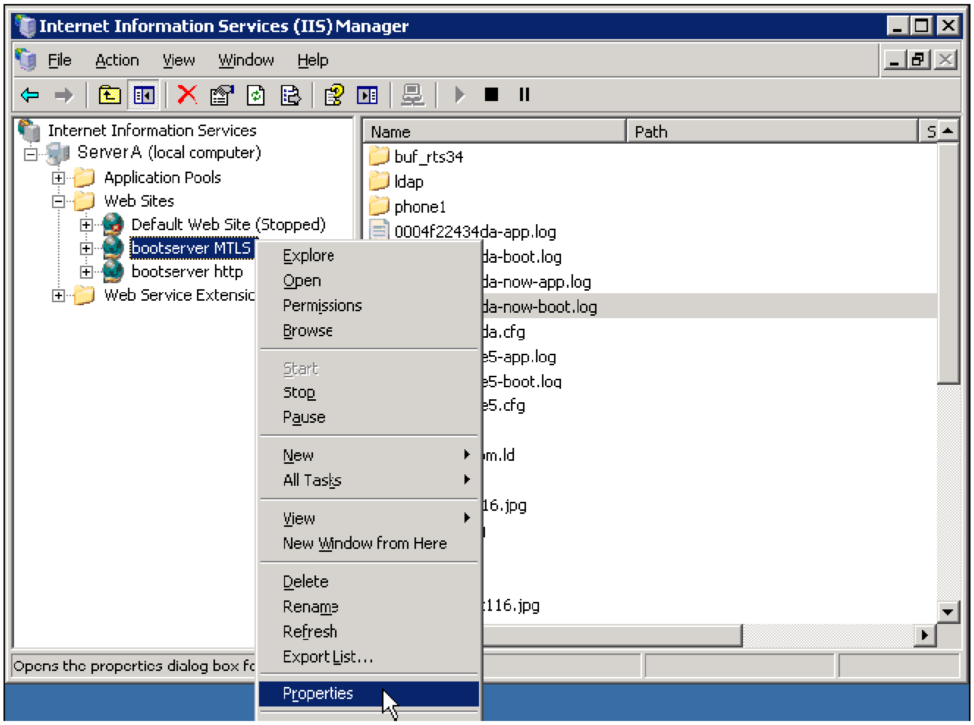
Note At this point, the Microsoft Certificate Authority will start to install. Microsoft Windows 2003 media may be required to complete the installation.

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

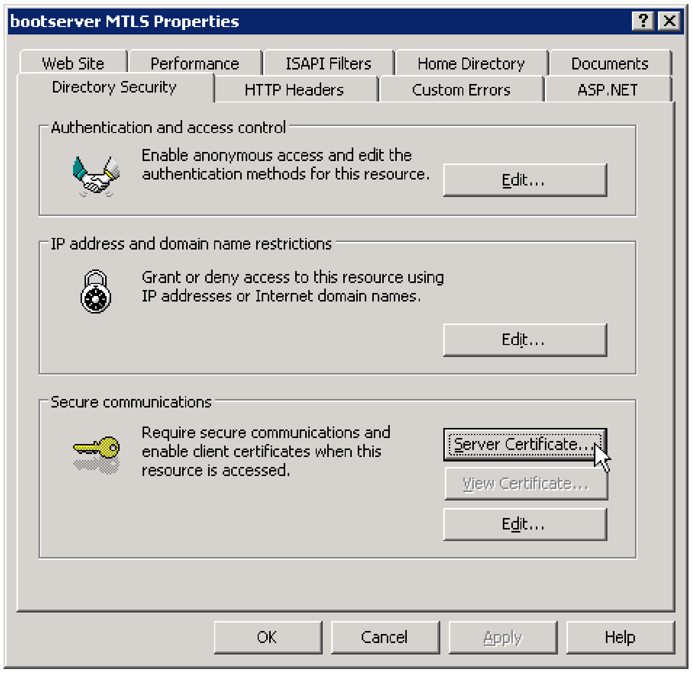
Note This step is not required if you use a certificate from a known CA.

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**.



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



bootserver MTLS Properties

Authentication and access control

Enable anonymous access and edit the authentication methods for this resource.

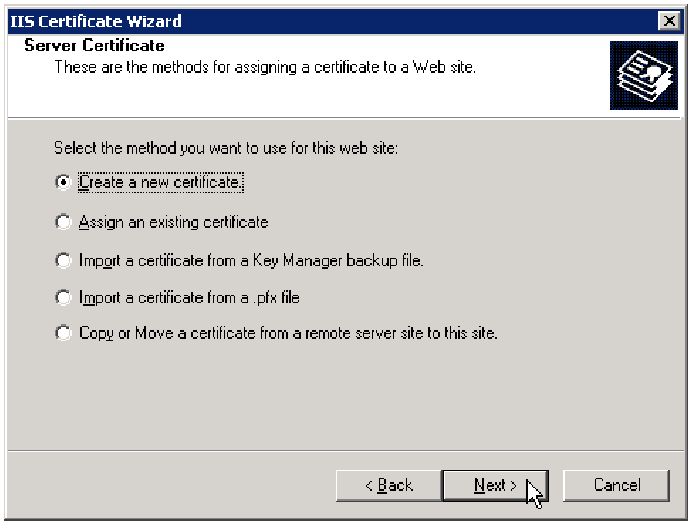
IP address and domain name restrictions

Grant or deny access to this resource using IP addresses or Internet domain names.

Secure communications

Require secure communications and enable client certificates when this resource is accessed.

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



IIS Certificate Wizard

Server Certificate

These are the methods for assigning a certificate to a Web site.

Select the method you want to use for this web site:

● Create a new certificate.

○ Assign an existing certificate

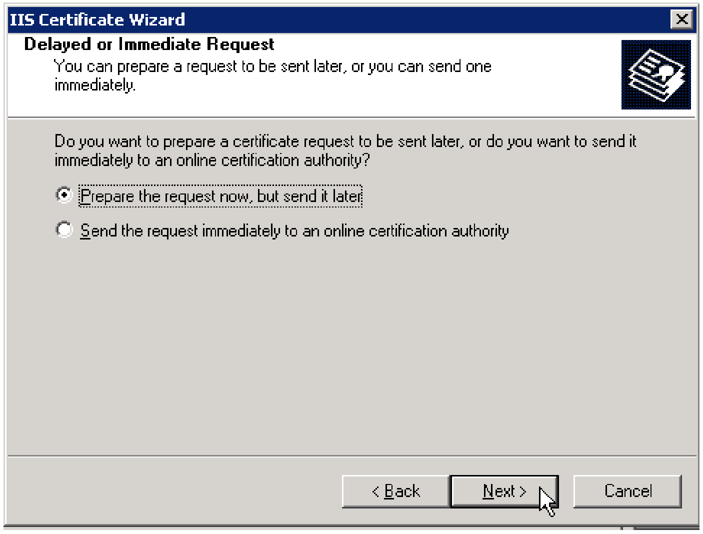
○ Import a certificate from a Key Manager backup file.

○ Import a certificate from a .pfx file

○ Copy or Move a certificate from a remote server site to this site.

4. From the IIS Certificate Wizard, do the following:

   – Click **Prepare the request now, but send it later**, and then click **Next**.



IIS Certificate Wizard

Delayed or Immediate Request

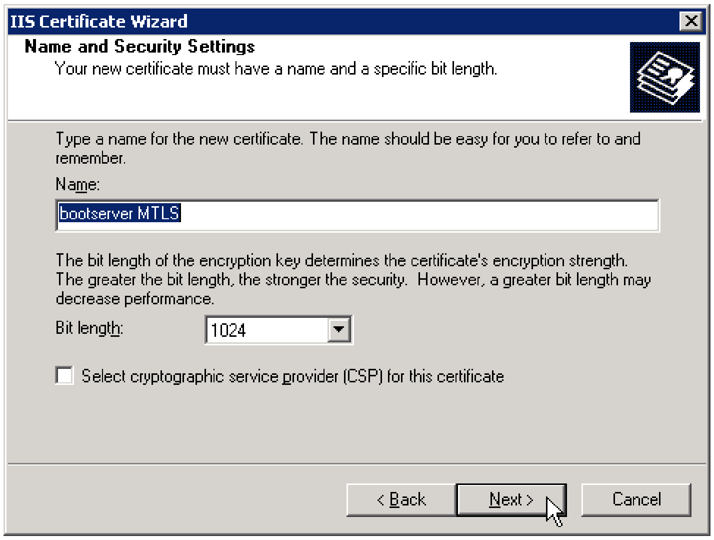
You can prepare a request to be sent later, or you can send one immediately.

Do you want to prepare a certificate request to be sent later, or do you want to send it immediately to an online certification authority?

● Prepare the request now, but send it later

○ Send the request immediately to an online certification authority

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



IIS Certificate Wizard

Name and Security Settings

Your new certificate must have a name and a specific bit length.

Type a name for the new certificate. The name should be easy for you to refer to and remember.

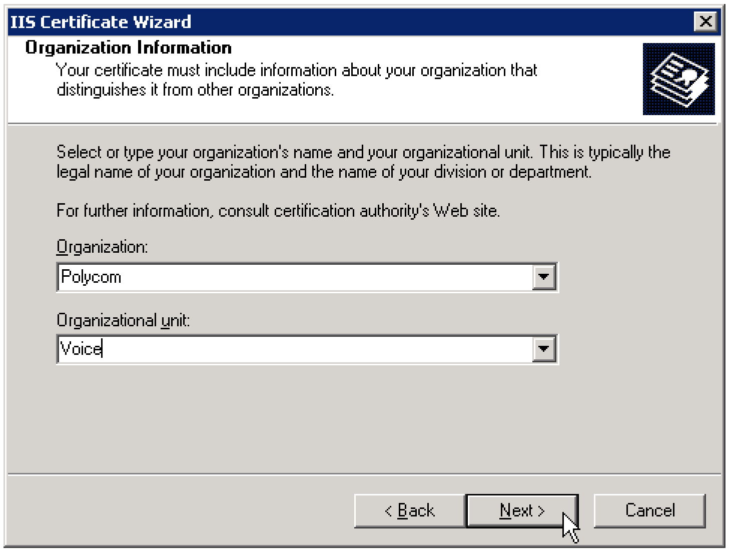
Name: bootserver MTLS

The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Bit length: 1024

□ Select cryptographic service provider (CSP) for this certificate

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


IIS Certificate Wizard

Organization Information

Your certificate must include information about your organization that distinguishes it from other organizations.

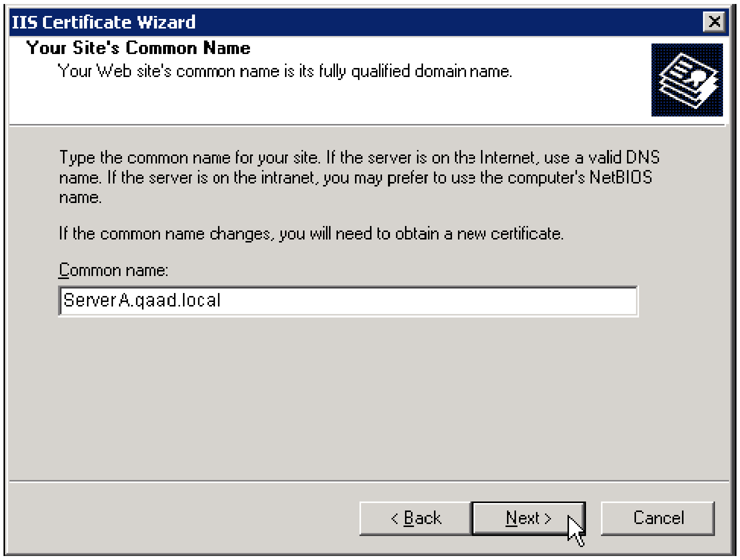
Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.

For further information, consult certification authority's Web site.

Organization: Polycom

Organizational unit: Voice

— 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**.


IIS Certificate Wizard

Your Site's Common Name

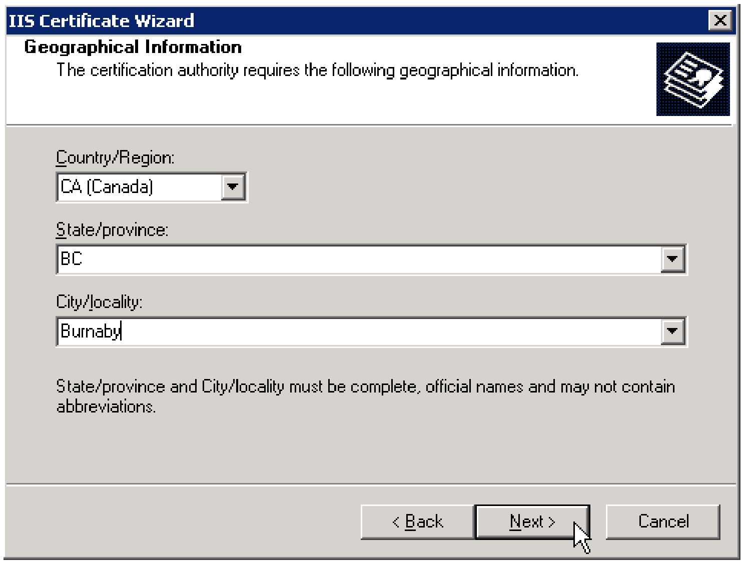
Your Web site's common name is its fully qualified domain name.

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.

Common name: ServerA.qaad.local

— Enter your location information, and then click **Next**.



IIS Certificate Wizard

Geographical Information

The certification authority requires the following geographical information.

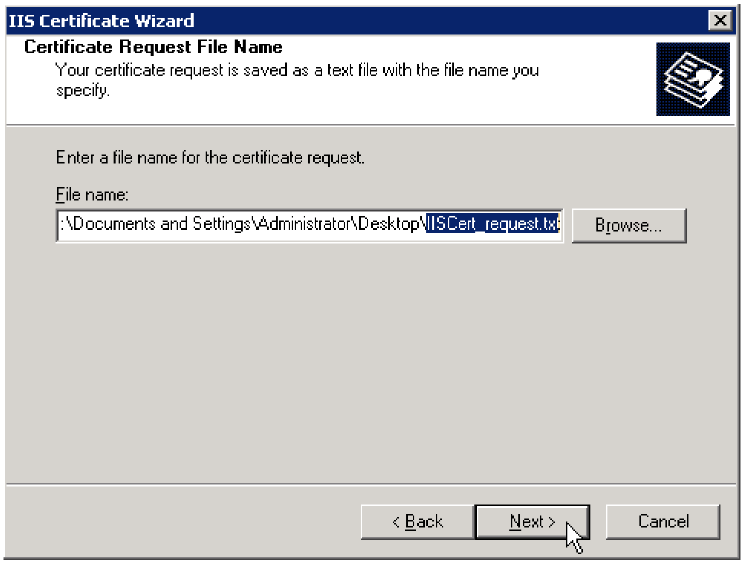
Country/Region: CA (Canada)

State/province: BC

City/locality: Burnaby

State/province and City/locality must be complete, official names and may not contain abbreviations.

— 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. Click **Next**.



IIS Certificate Wizard

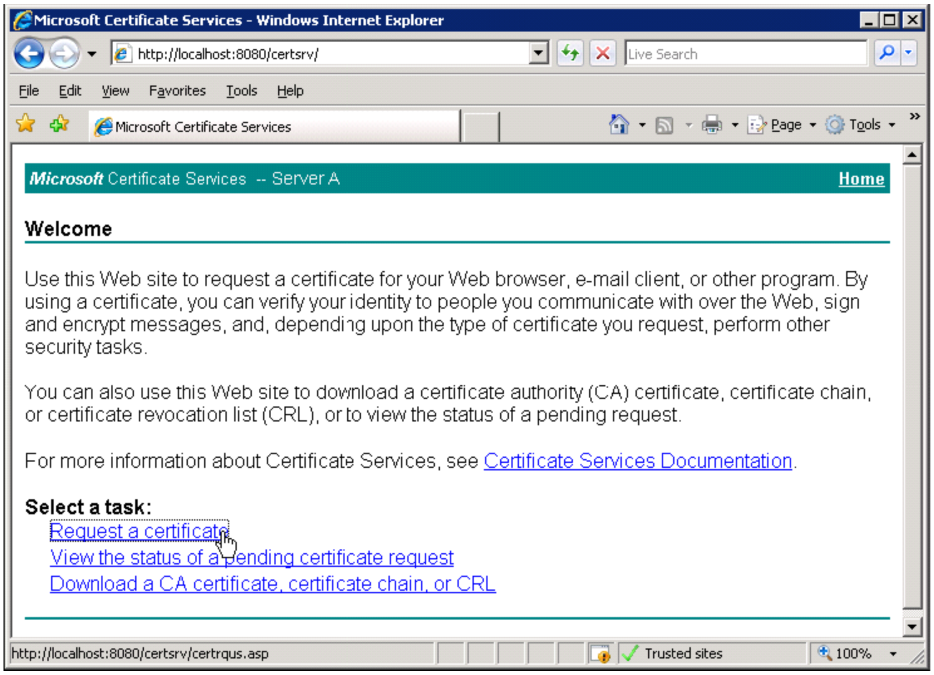
Certificate Request File Name

Your certificate request is saved as a text file with the file name you specify.

Enter a file name for the certificate request.

File name: :\Documents and Settings\Administrator\Desktop\IISCert_request.txt

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**.



Microsoft Certificate Services - Windows Internet Explorer
http://localhost:8080/certsrv/
Live Search
File Edit View Favorites Tools Help
Microsoft Certificate Services
Page Tools

Microsoft Certificate Services -- Server A Home

Welcome

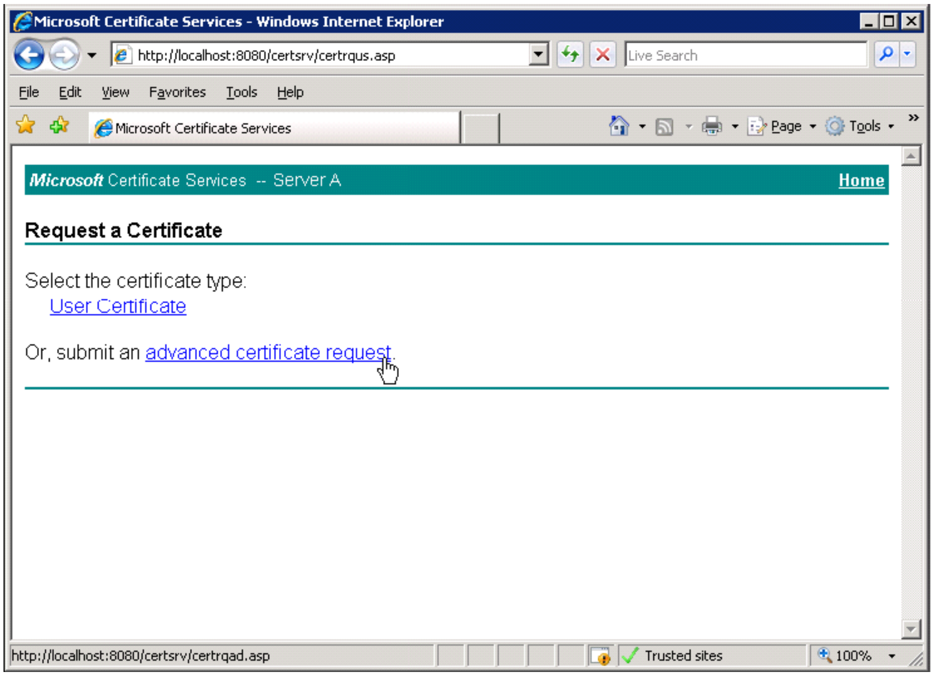
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

6. Click **advanced certificate request**.



Microsoft Certificate Services - Windows Internet Explorer
http://localhost:8080/certsrv/certrqus.asp
Live Search
File Edit View Favorites Tools Help
Microsoft Certificate Services
Page Tools

Microsoft Certificate Services -- Server A Home

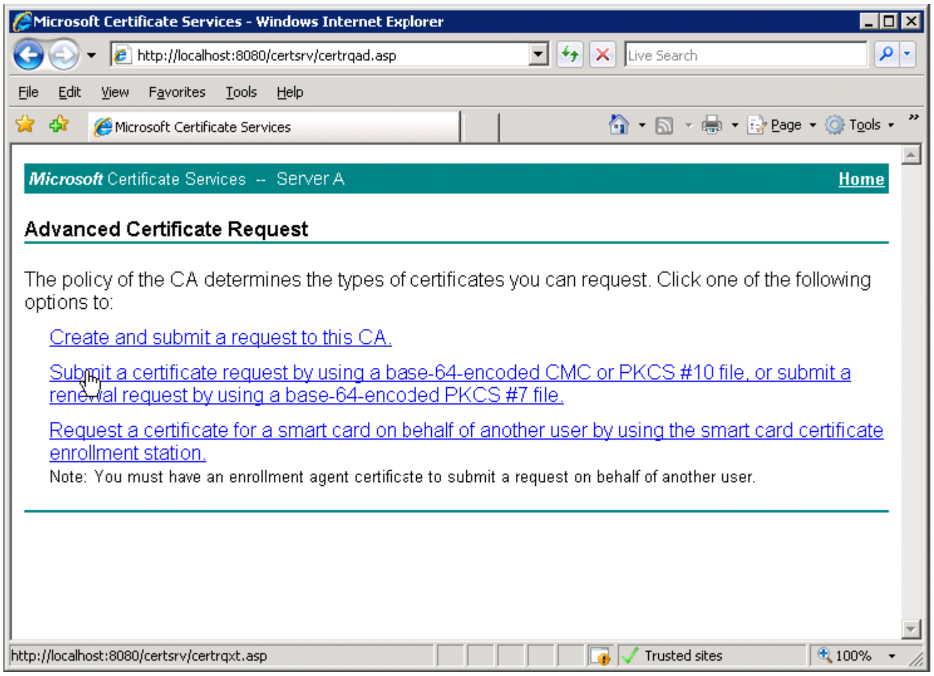
Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

http://localhost:8080/certsrv/certrqad.asp
Trusted sites
100%

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**.


Microsoft Certificate Services - Windows Internet Explorer
http://localhost:8080/certsrv/certrqad.asp
Live Search
File Edit View Favorites Tools Help
Microsoft Certificate Services
Page
Tools
Microsoft Certificate Services -- Server A
Home
http://localhost:8080/certsrv/certrqxt.asp
Trusted sites
100%

Advanced Certificate Request

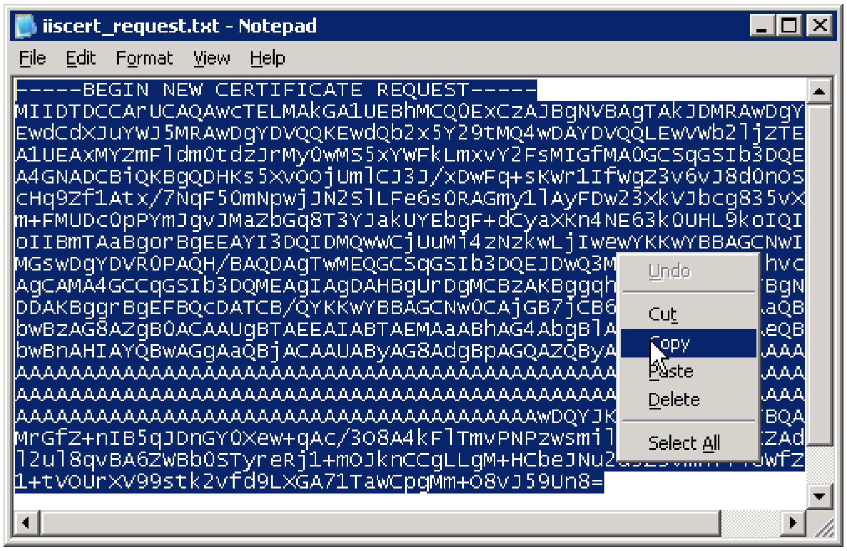
The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

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.

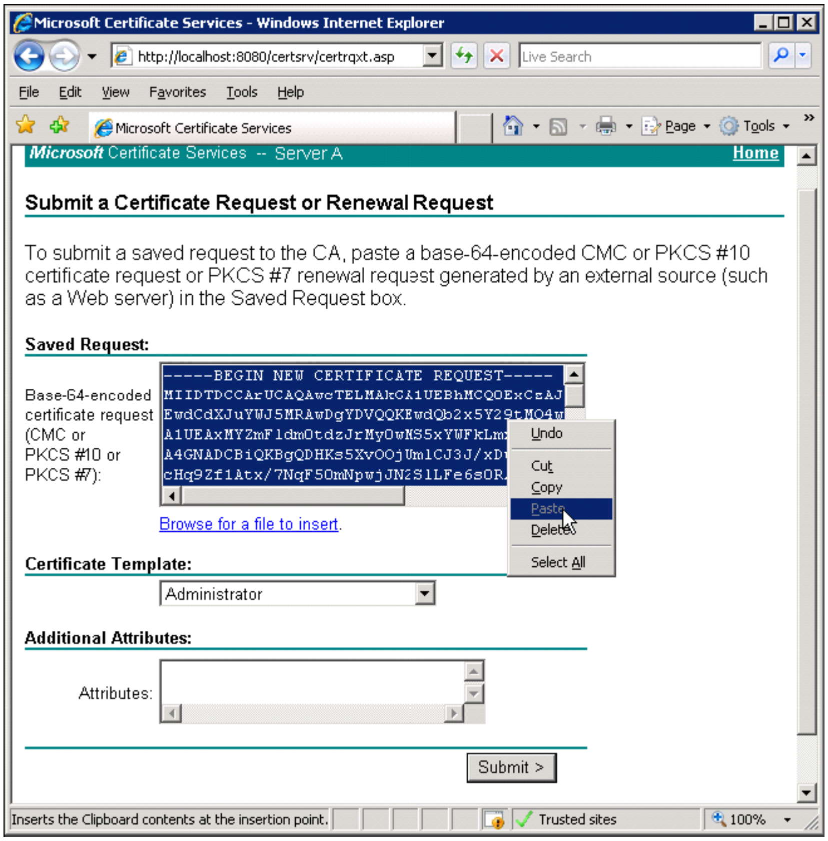
Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.
Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

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



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDTDCCArUCAQAwcTELMAkGA1UEBhMCQ0ExCzAJBgNVBAgTAkJDMRAwDgY
EwdCdXJuYWJ5MRAwDgYDVQQKEwdQb2x5Y29tMQ4wDAYDVQQLEwVwb2ljZTE
A1UEAxMYZmFldm0tdzJrMy0wMS5xYWFkLmxvY2FsMIGfMA0GCSqGSIb3DQE
A4GNADCBiQKBgQDHKs5XvOOjUmlCJ3J/xDwFq+sKWr1IfwgZ3v6vJ8d0noS
cHq9Zf1Atx/7NqF50mNpwjJN2SlLFe6s0RAGmy1lAyFDw23XkVJbcg835vX
m+FMUDc0pPYmJgvJMaZbGq8T3YJakUYEbgF+dCyaXKn4NE63k0UHL9koIQI
oIIBmTAaBgorBgEEAYI3DQIDMQwWCjUuMi4zNzkwLjIwewYKKwYBBAGCNwI
MGswDgYDVR0PAQH/BAQDAgTwMEQGCSqGSIb3DQEJDwQ3M          hvc
AgCAMA4GCCqGSIb3DQMEAgIAgDAHBgUrDgMCBzAKBggqh          BgN
DDAKBggrBgEFBQcDATCB/QYKKwYBBAGCNw0CAjGB7jCB6          aQB
bwBzAG8AZgB0ACAAUgBTAEEAIABTAEMAaABhAG4AbgBlA          eQB
bwBnAHIAYQBwAGgAaQBjACAAUAByAG8AdgBpAGQAZQByA          AAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA          AAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA          AAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAWDQYJK          BQA
MrGfZ+nIB5qJDnGY0Xew+qAc/308A4kFlTmvPNPzwsmil          ZAd
l2ul8qvBA6ZWBb0STyreRj1+mOJknCCgLLgM+HCbeJNu2          wfZ
1+tvOUrxV99stk2vfd9LXGA71TaWCpqMm+08vJ59Un8=
```

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


Microsoft Certificate Services - Windows Internet Explorer
http://localhost:8080/certsrv/certrqxt.asp
Live Search
File Edit View Favorites Tools Help
Microsoft Certificate Services
Page Tools
Microsoft Certificate Services -- Server A
Home
Undo
Cut
Copy
Paste
Delete
Select All
Submit >
Inserts the Clipboard contents at the insertion point.
Trusted sites
100%

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

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

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDTDCCArUCAQAwcTELMAkGA1UEBhMCQ0ExCzAJ
EwdCdXJuYWJ5MRAwDgYDVQQKEwdQb2x5Y29tMQ4w
A1UEAxMYZmF1dm0tdzJrMy0wNS5xYWFkLm
A4GNADCBiQKBgQDHKs5XvOOjUmlCJ3J/xDu
cHq9Zf1Atx/7NqF5OmNpwjJN2S1LFe6sOR
```

Browse for a file to insert.

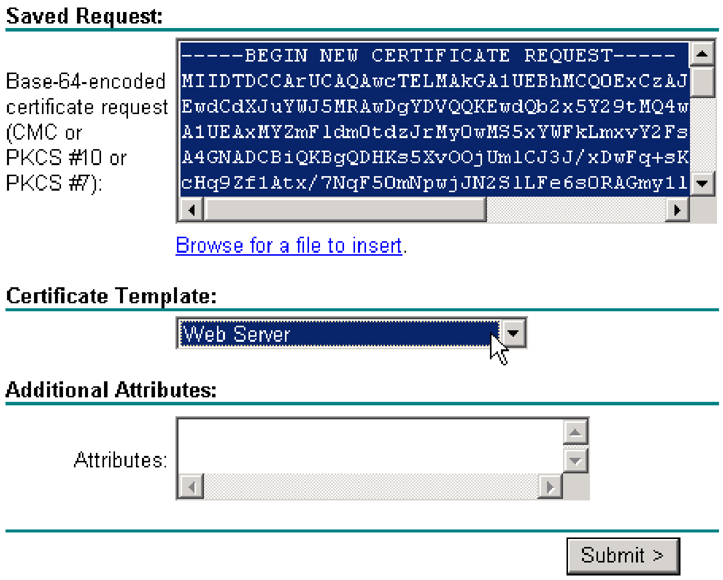
Certificate Template:

Administrator

Additional Attributes:

Attributes:

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-----
MIIDTDCCArUCAQAwcTELMAkGA1UEBhMCQ0ExCzAJ
EwdCdXJuYWJ5MRAwDgYDVQQKEwdQb2x5Y29tMQ4w
A1UEAxMYZmF1dm0tdzJrMy0wMS5xYWFkLmxvY2Fs
A4GNADCBiQKBgQDHKs5XvO0jUm1CJ3J/xDwFq+sK
cHq9Zf1Atx/7NqF50mNpwjJN2S1LFe6s0RAGmy11
```

Browse for a file to insert.

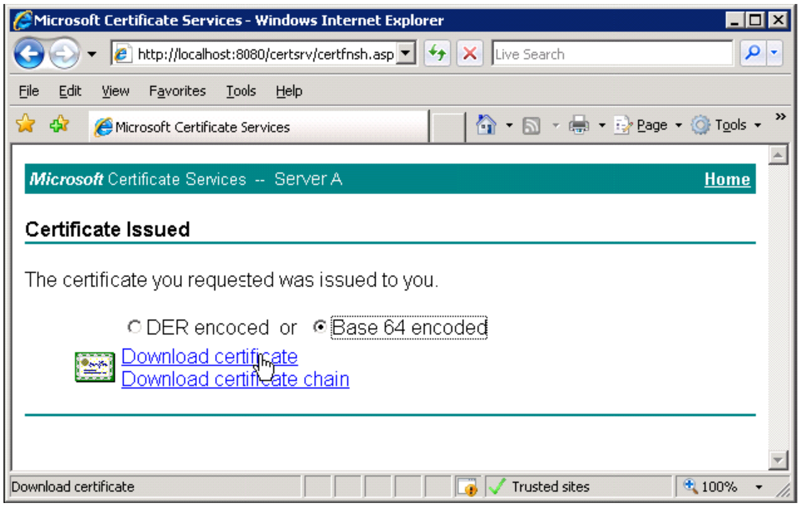
Certificate Template:

Web Server

Additional Attributes:

Attributes:

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



Microsoft Certificate Services - Windows Internet Explorer
http://localhost:8080/certsrv/certfnsh.asp
Live Search
File Edit View Favorites Tools Help
Microsoft Certificate Services
Page Tools

Microsoft Certificate Services -- Server A **Home**

Certificate Issued

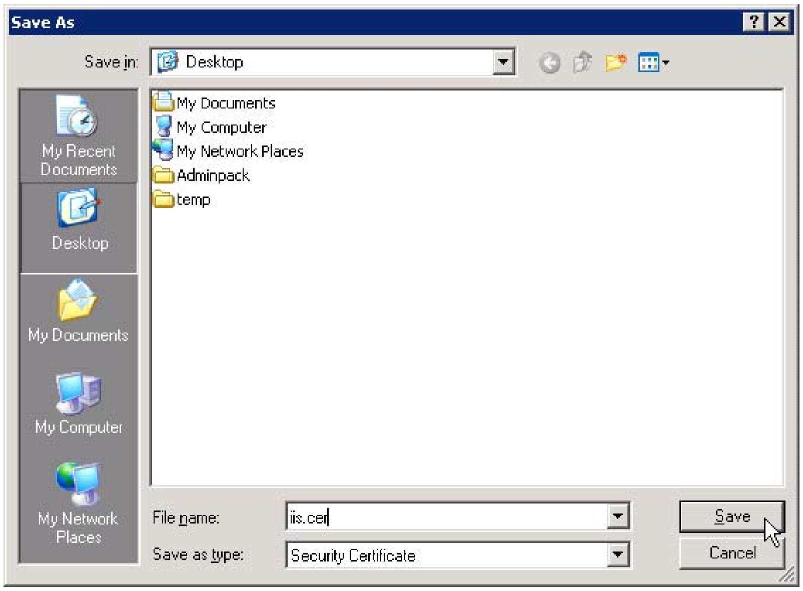
The certificate you requested was issued to you.

○ DER encoced or ● Base 64 encoded

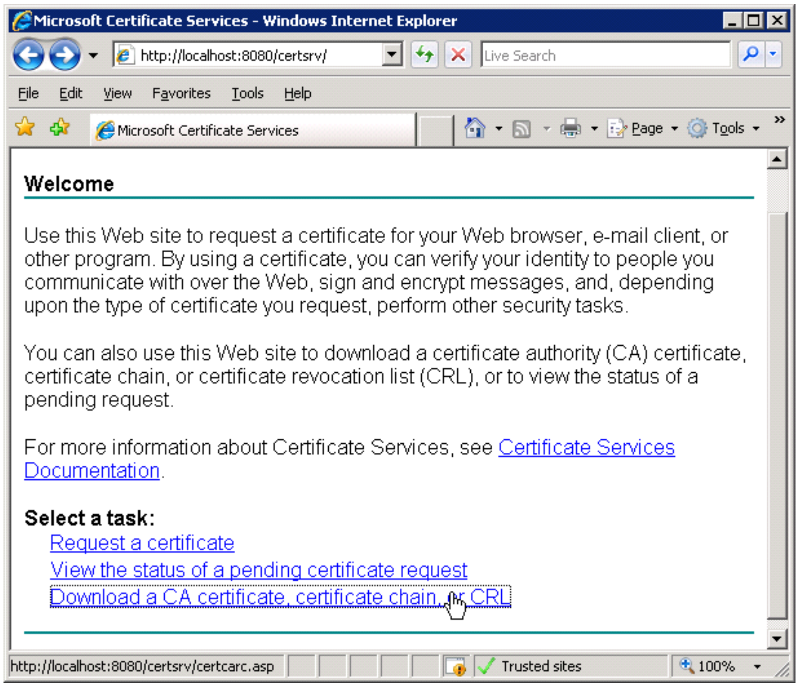
Download certificate
Download certificate chain

Download certificate
Trusted sites
100%

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 on page 33).



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


Microsoft Certificate Services - Windows Internet Explorer
http://localhost:8080/certsrv/
Live Search
File Edit View Favorites Tools Help
Microsoft Certificate Services
Page Tools
http://localhost:8080/certsrv/certcarc.asp
Trusted sites
100%

Welcome

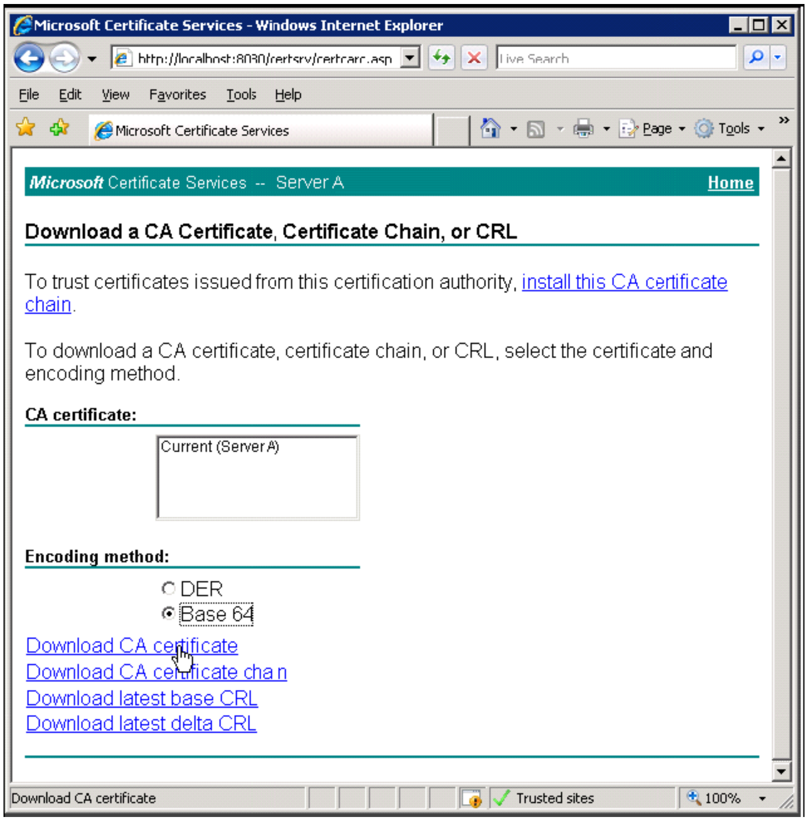
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

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


Microsoft Certificate Services - Windows Internet Explorer
http://localhost:8030/certsrv/certcarc.asp
Live Search
File Edit View Favorites Tools Help
Microsoft Certificate Services
Page
Tools

Microsoft Certificate Services -- Server A **Home**

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

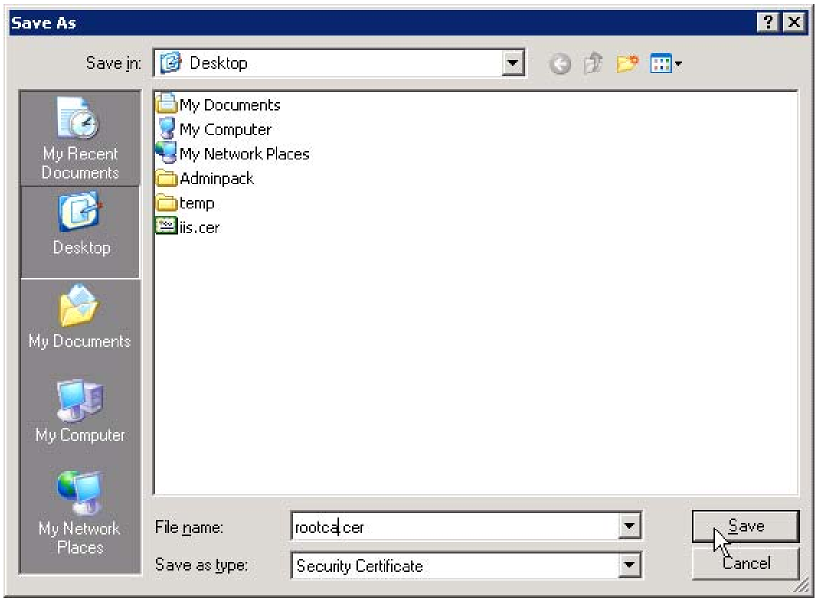
Current (Server A)

Encoding method:

○ DER
● Base 64

Download CA certificate
Download CA certificate cha n
Download latest base CRL
Download latest delta CRL

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 on page 36).



File name: rootca.cer

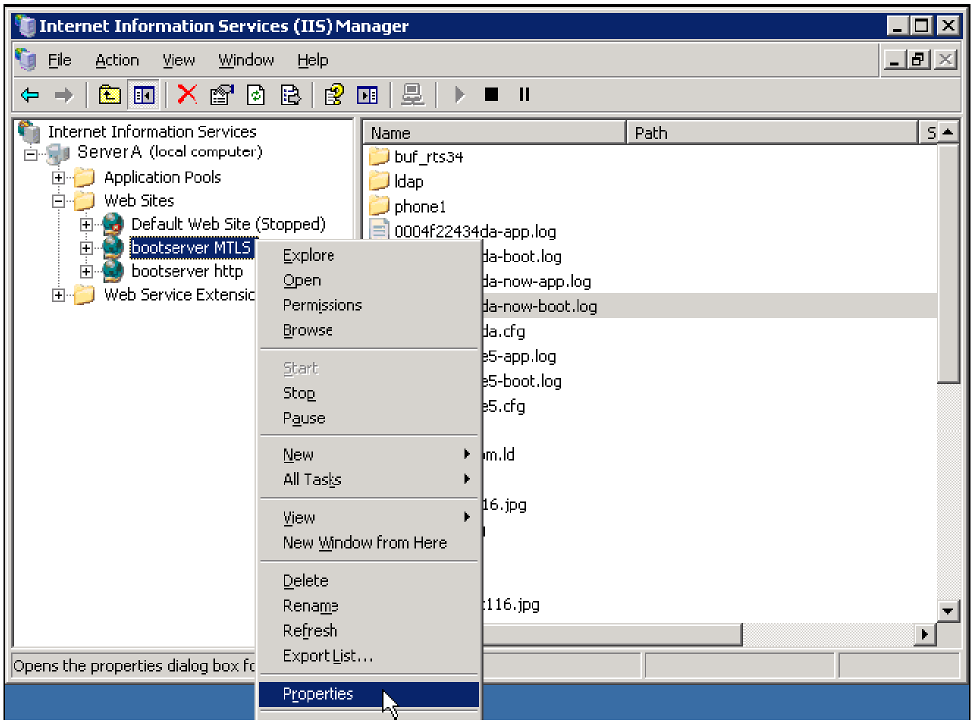
Save as type: Security Certificate

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

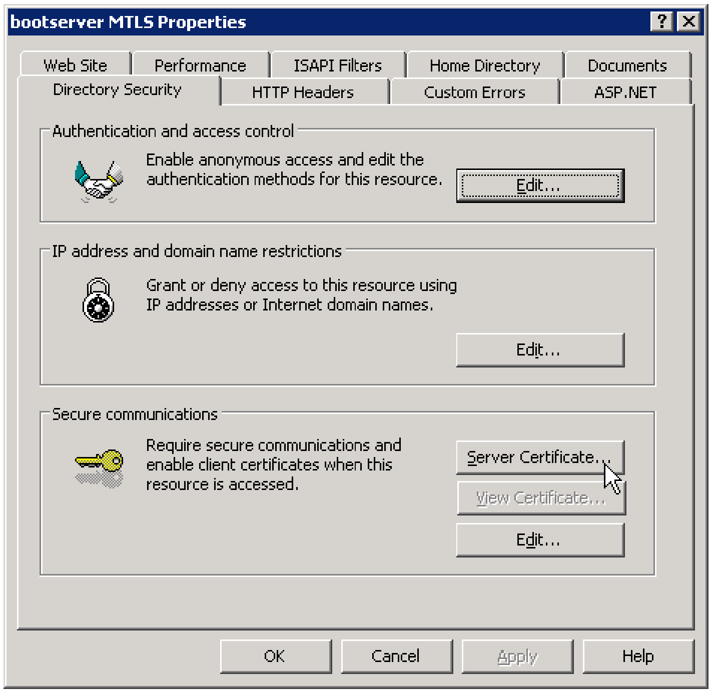
Installing the Server Certificate on the IIS Server

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**.



bootserver MTLS Properties

Authentication and access control

Enable anonymous access and edit the authentication methods for this resource.

IP address and domain name restrictions

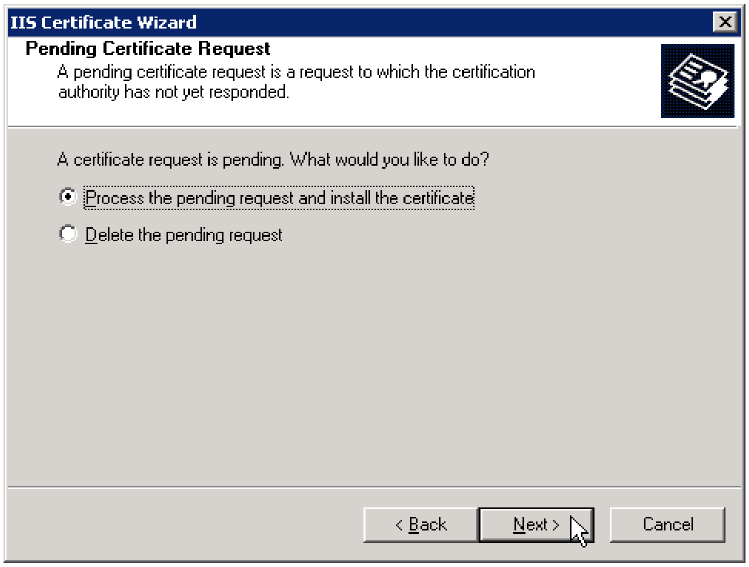
Grant or deny access to this resource using IP addresses or Internet domain names.

Secure communications

Require secure communications and enable client certificates when this resource is accessed.

3. From the IIS Certificate Wizard window, do the following:

– Click **Process the pending request and install the certificate**, and then click **Next**.



IIS Certificate Wizard

Pending Certificate Request

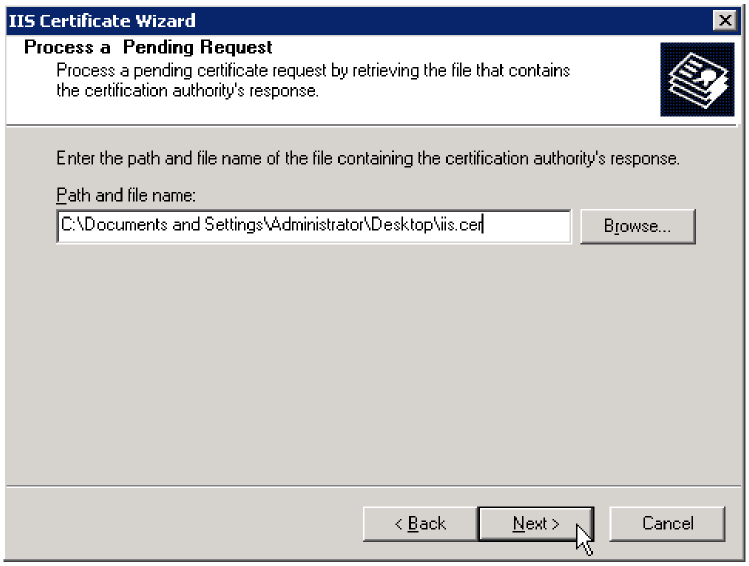
A pending certificate request is a request to which the certification authority has not yet responded.

A certificate request is pending. What would you like to do?

● Process the pending request and install the certificate

○ Delete the pending request

- Enter the location (for example, your desktop) of the IIS server certificate you created in a previous section (see Creating the IIS Server Self-Signed Certificate for the IIS HTTPS Server on page 21), and then click **Next**.



IIS Certificate Wizard

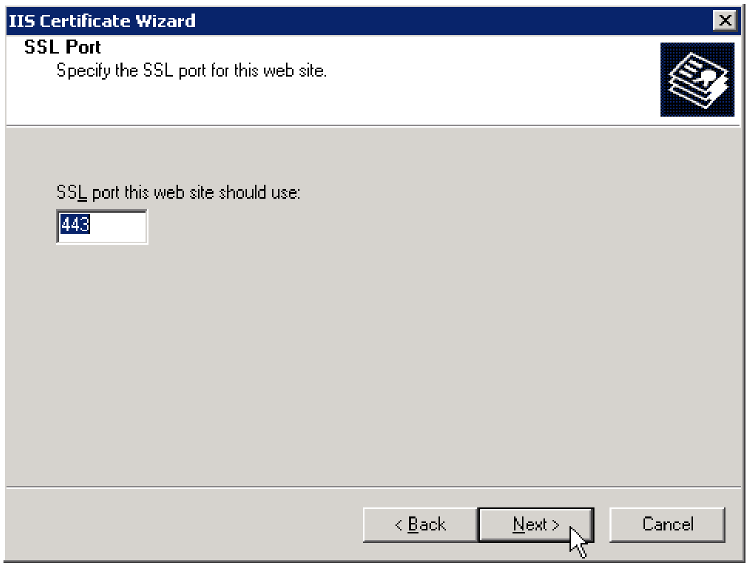
Process a Pending Request

Process a pending certificate request by retrieving the file that contains the certification authority's response.

Enter the path and file name of the file containing the certification authority's response.

Path and file name: C:\Documents and Settings\Administrator\Desktop\iis.cer

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



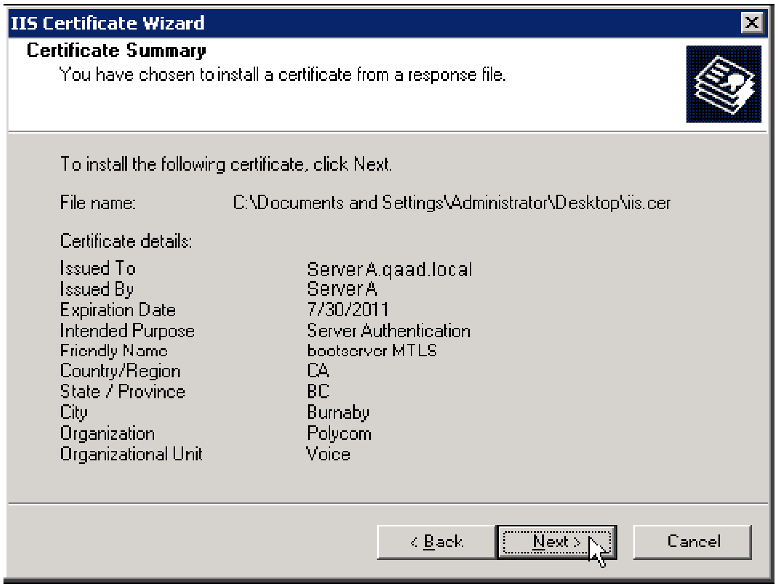
IIS Certificate Wizard

SSL Port

Specify the SSL port for this web site.

SSL port this web site should use: 443

- 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.



IIS Certificate Wizard

Certificate Summary

You have chosen to install a certificate from a response file.

To install the following certificate, click Next.

File name: C:\Documents and Settings\Administrator\Desktop\iis.cer

Certificate details:

Issued To	ServerA.qaad.local
Issued By	ServerA
Expiration Date	7/30/2011
Intended Purpose	Server Authentication
Friendly Name	bootserver MTLS
Country/Region	CA
State / Province	BC
City	Burnaby
Organization	Polycom
Organizational Unit	Voice

The IIS server certificate is installed in the IIS HTTPS virtual server.

Installing the Root CA Server Certificate on the Polycom Phone

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 a previous section (see Creating the IIS Server Self-Signed Certificate for the IIS HTTPS Server on page 21).
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 the **Enter** soft key.
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 phone, select **Administration Settings** > **Network Configuration** > **Server Menu**.

5. In the Server Menu window, do the following:
   - For **Server Type**, select **HTTP** (so that you can download the root CA certificate from your boot server), and then press the **OK** soft key.
   - For **Server Address**, enter the server address of your HTTP boot server, and then press the **OK** soft key.
   - For **Server User**, enter the user name to your HTTP boot server, and then press the **OK** soft key.
   - For **Server Password**, enter the password to your HTTP boot server, and then press the **OK** soft key.
6. Do one of the following:
   - If you have a SoundPoint IP phone, press the **Exit** soft key twice, and then save the new configuration.
   - If you have a SoundStation IP or VVX 1500 phone, press the **Back** soft key 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 the **Enter** soft key.
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 phone, select **Administration Settings** > **SSL Security** > **CA Certificates** > **Install Custom CA Cert**.
10. In the Install Custom CA Certificate window, enter the location of the certificate for your root CA server, and then press the **Enter** soft key.

    The phone will download the certificate and display the MD5 fingerprint.
11. To accept the certificate, press the **Accept** soft key.
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 phone, press the **Back** soft key, 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

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 the **Enter** soft key.
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 phone, select **Administration Settings** > **Network Configuration** > **Server Menu**.
17. In the Server Menu window, for the **Server Type**, select **HTTPS**, and then press the **OK** soft key.
18. Do one of the following:
    - If you have a SoundPoint IP phone, press the **Exit** soft key twice, and then save the new configuration.
    - If you have a SoundStation IP or VVX 1500 phone, press the **Back** soft key twice, and then save the new configuration.

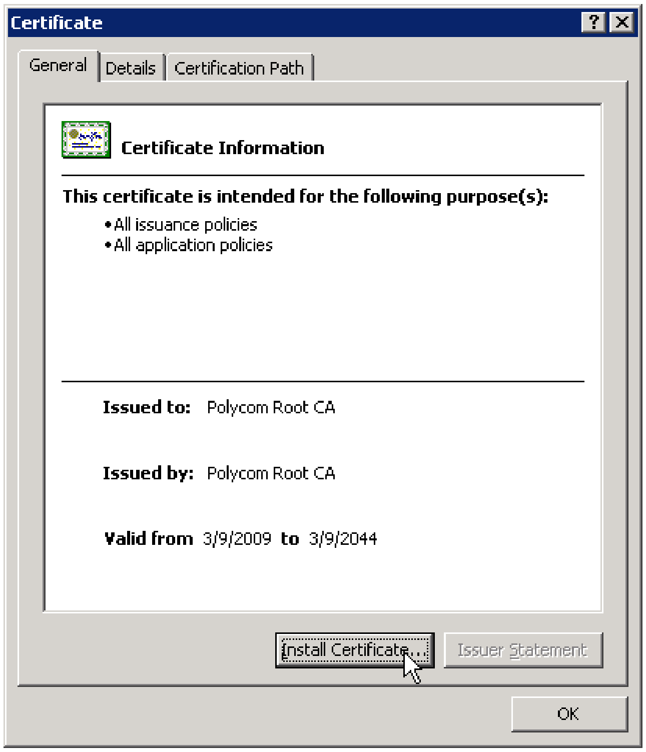
Installing the Polycom Root CA Certificate on the Microsoft Certificate Authority Server

Note This step is not required if you use a certificate from a known CA.

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

1. Access the Polycom Root CA Certificate from http://pki.polycom.com/pki/Polycom%20Root%20CA.crt.

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



Certificate Information

This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

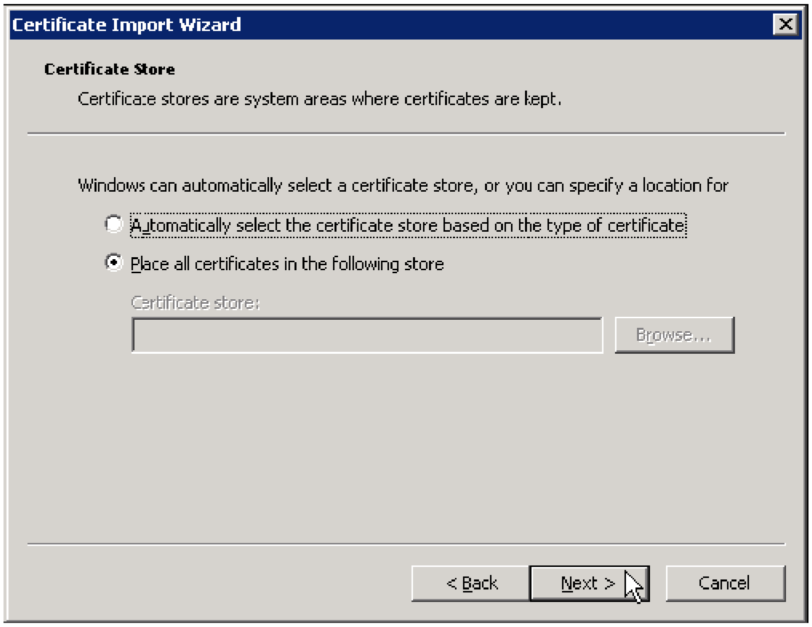
Issued to: Polycom Root CA

Issued by: Polycom Root CA

Valid from 3/9/2009 **to** 3/9/2044

3. From the Certificate Import Wizard, do the following:

   – Click **Place all certificates in the following store**, and then click **Next**.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

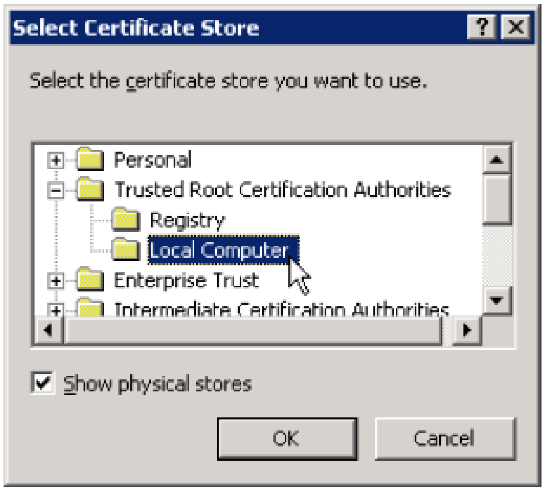
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

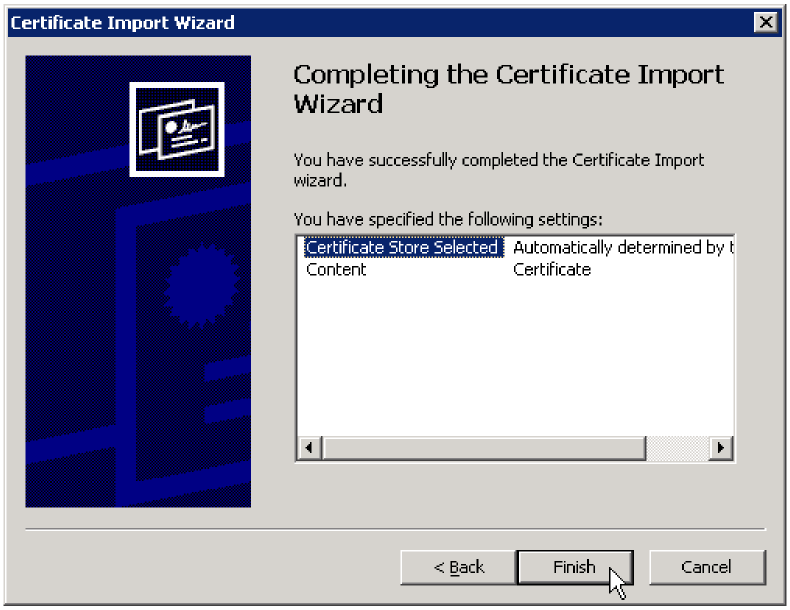
- From the Select Certificate Store window, double-click **Trusted Root Certification Authorities**, and then click **Local Computer**. Then, select the **Show Physical Stores** check box, and then press **OK**.

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



Select Certificate Store
Select the certificate store you want to use.
Personal
Trusted Root Certification Authorities
Registry
Local Computer
Enterprise Trust
Intermediate Certification Authorities
☑ Show physical stores
OK
Cancel

- Click **Finish**.



Certificate Import Wizard

Completing the Certificate Import Wizard

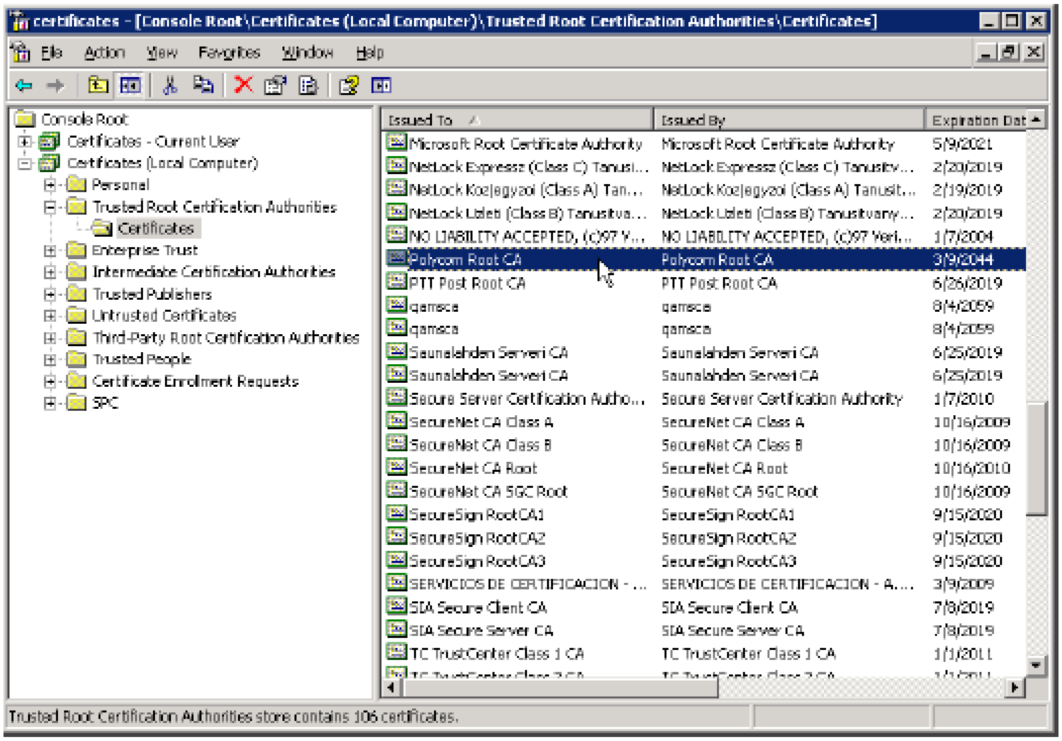
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	Certificate

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.


certificates - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Certificate Enrollment Requests
SPC

Issued To	Issued By	Expiration Dat
Microsoft Root Certificate Authority	Microsoft Root Certificate Authority	5/9/2021
NetLock Expressz (Class C) Tanusi...	NetLock Expressz (Class C) Tanusitv...	2/20/2019
NetLock Kozjegyzoi (Class A) Tan...	NetLock Kozjegyzoi (Class A) Tanusit...	2/19/2019
NetLock Uzleti (Class B) Tanusitva...	NetLock Uzleti (Class B) Tanusitvany...	2/20/2019
NO LIABILITY ACCEPTED, (c)97 V...	NO LIABILITY ACCEPTED, (c)97 Veri...	1/7/2004
Polycom Root CA	Polycom Root CA	3/9/2044
PTT Post Root CA	PTT Post Root CA	6/26/2019
qamsca	qamsca	8/4/2059
qamsca	qamsca	8/4/2059
Saunalahden Serveri CA	Saunalahden Serveri CA	6/25/2019
Saunalahden Serveri CA	Saunalahden Serveri CA	6/25/2019
Secure Server Certification Autho...	Secure Server Certification Authority	1/7/2010
SecureNet CA Class A	SecureNet CA Class A	10/16/2009
SecureNet CA Class B	SecureNet CA Class B	10/16/2009
SecureNet CA Root	SecureNet CA Root	10/16/2010
SecureNet CA SGC Root	SecureNet CA SGC Root	10/16/2009
SecureSign RootCA1	SecureSign RootCA1	9/15/2020
SecureSign RootCA2	SecureSign RootCA2	9/15/2020
SecureSign RootCA3	SecureSign RootCA3	9/15/2020
SERVICIOS DE CERTIFICACION - ...	SERVICIOS DE CERTIFICACION - A....	3/9/2009
SIA Secure Client CA	SIA Secure Client CA	7/8/2019
SIA Secure Server CA	SIA Secure Server CA	7/8/2019
TC TrustCenter Class 1 CA	TC TrustCenter Class 1 CA	1/1/2011
TC TrustCenter Class 2 CA	TC TrustCenter Class 2 CA	1/1/2011

Trusted Root Certification Authorities store contains 106 certificates.

Note

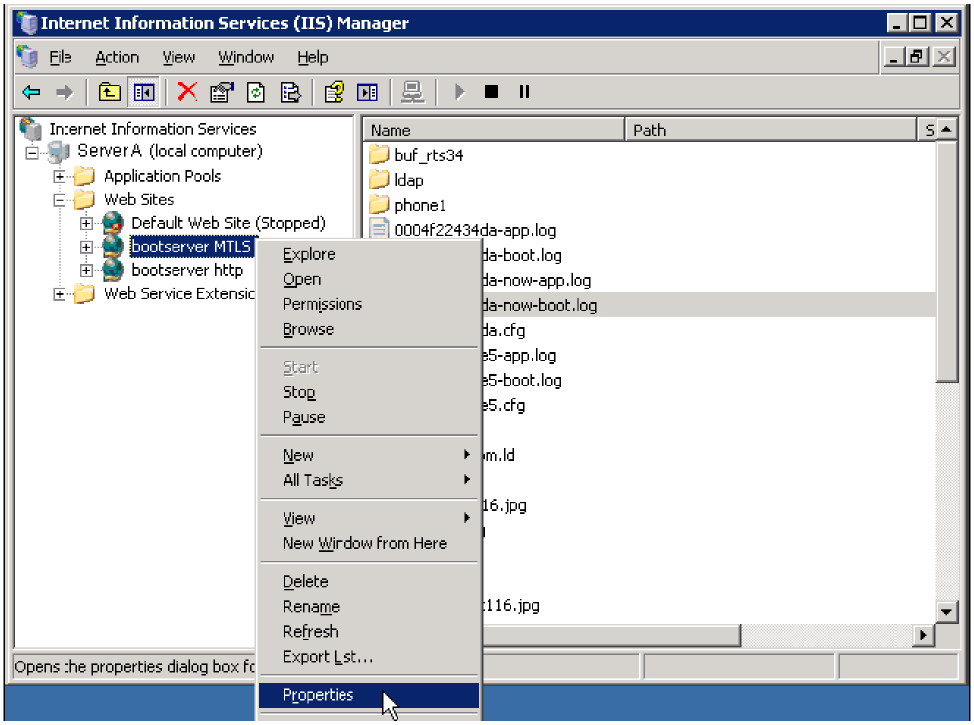
If your root CA does not recognize the Polycom intermediate CAs, you may have to install the intermediate certificates, or configure Microsoft to automatically download the intermediate certificates. For more information, see Troubleshooting on page 45.

Enabling Mutual TLS on the IIS Server

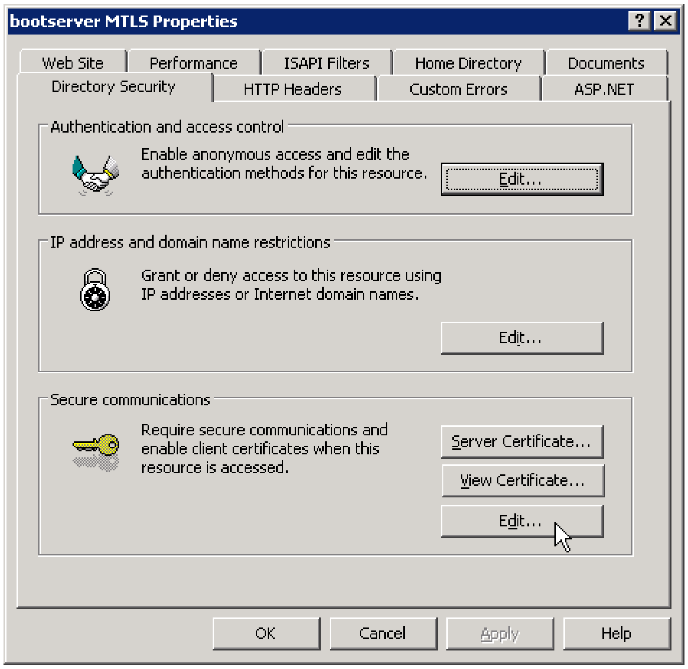
You must set the IIS server to require a Client Certificate to enable mutual TLS on the server.

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**.


bootserver MTLS Properties

Authentication and access control

Enable anonymous access and edit the authentication methods for this resource.

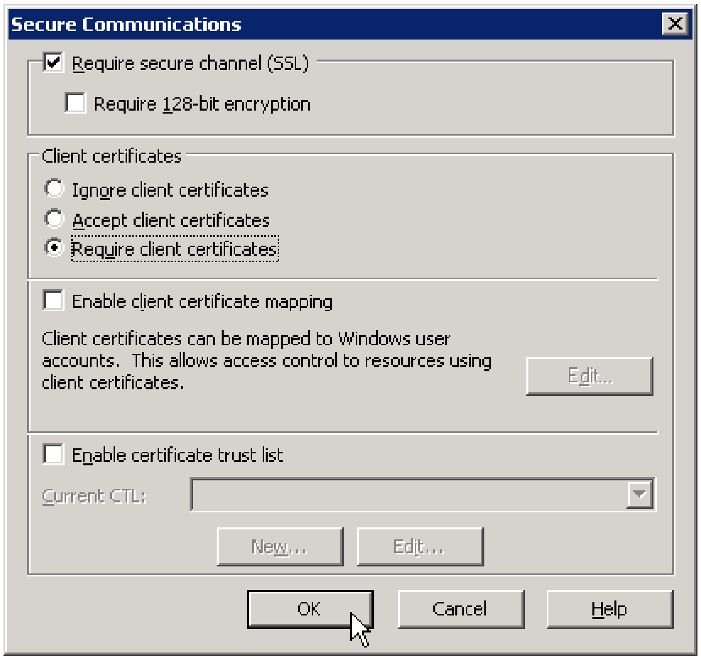
IP address and domain name restrictions

Grant or deny access to this resource using IP addresses or Internet domain names.

Secure communications

Require secure communications and enable client certificates when this resource is accessed.

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**.



Secure Communications

☑ Require secure channel (SSL)

□ Require 128-bit encryption

Client certificates

○ Ignore client certificates

○ Accept client certificates

● Require client certificates

□ Enable client certificate mapping

Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.

□ Enable certificate trust list

Current CTL:

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

Issue	Do the following...

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, as shown below:
	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, as shown below:
	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
	Note: The above 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, as shown below:
	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.

Issue	Do the following...
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 http://support.microsoft.com/kb/968730.
Intermediate certificates are not downloaded to complete a certificate chain by default.	See the topic "Intermediate Certificates Are Not Downloaded to Complete a Certificate Chain" at http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/77cf4a99-9e0e-42be-8c2e-eaa4cb24c200.mspx?mfr=true. 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, go to http://support.microsoft.com/kb/820129.

Additional Information

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

- *Administrator's Guide for the Polycom SoundPoint IP/SoundStation IP/VVX Family*, at www.polycom.com/voicedocumentation
- Technical Bulletin 46792, *Best Practices when Using HTTP and HTTPS Provisioning on Polycom SoundPoint IP, SoundStation IP, and VVX Phones*, at http://www.polycom.com/usa/en/support/voice/soundpoint_ip/VoIP_Technical_Bulletins_pub.html
- *Digest authentication and Advanced Digest authentication in Windows Server 2003*, at http://support.microsoft.com/default.aspx?scid=kb;EN-US;824032

Trademark Information