AD Summation

AccessData

Installation and Upgrade Guide

WebBlaze

Version 3.1

Published: September 2010

COPYRIGHT INFORMATION

© 2010 AccessData, LLC.

All rights reserved.

The information contained in this document represents the current view of AD Summation on the issues discussed as of the date of publication. Because AD Summation must respond to changing market conditions, it should not be interpreted to be a commitment on the part of AD Summation, and AD Summation cannot guarantee the accuracy of any information presented after the date of publication. This document is for informational purposes only. AD SUMMATION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) or for any purpose, without the express written permission of AD Summation.

AD Summation may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document; except as expressly provided in any written license agreement from AD Summation, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

AD Summation, iBlaze, Blaze, Enterprise, and WebBlaze are trademarks of AD Summation in the United States and/or other countries. Microsoft, Windows, PowerPoint, and Outlook are registered trademarks of Microsoft Corporation in the United States and/or other countries. Adobe, Acrobat, and Reader are registered trademarks, and Distiller is a trademark, of Adobe Systems Incorporated. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

AD Summation
425 Market Street, 7th Floor
San Francisco, CA 94105 USA

Contents

INTRODUCTION 1

Audience 1

Styles Used in This Document 1

RECOMMENDED SPECIFICATIONS AND PREREQUISITES 2

AD Summation WebBlaze Recommended Specifications 2

Prerequisite Checklist 2

INSTALLING AD SUMMATION WEBBLAZE 4

Network Topology Considerations 4

IIS Service Setup 7

Web Server Security Considerations 8

Setting Up a DNS Entry 9

Installing an SSL Certificate 9

Configuring a WebBlaze Service Account 9

AD Summation WebBlaze Installation 11

Securing AD Summation WebBlaze 15

UPGRADING AD SUMMATION WEBBLAZE 25

Introduction

This guide describes how to install and upgrade AD Summation WebBlaze.

For clarity, this guide is broken into two sections as noted below:

- For information on installing AD Summation WebBlaze, see Installing AD Summation WebBlaze.
- For information on upgrading AD Summation WebBlaze, see Upgrading AD Summation WebBlaze.

AUDIENCE

This document is intended for AD Summation administrators.

STYLES USED IN THIS DOCUMENT

This document provides a number of visual cues to help guide you. The following styles are used in this document:

Italicized Text – Italicized text indicates a new term or a term that is specific to AD Summation products. The first time that a new term is used, it is italicized and accompanied by a definition.

Italicized text also indicates the title of another document or section within this document.

Bold Text – Bold text indicates an item that is found on the AD Summation product interface, such as a menu option, a window, a field, or a dialog box.

Underlined Text: Underlined text indicates a link to a cross-referenced document containing further information on a subject.

NOTE: Notes call attention to supplemental yet important information about the topics covered in this document. Notes also provide suggestions on how to work more effectively with AD Summation products.

WARNING! Warnings call attention to actions that you should take (or avoid) to ensure data quality and/or successful operation of AD Summation products.

Recommended Specifications and Prerequisites

WEBBLAZE SERVER RECOMMENDED SPECIFICATIONS

- Processor – 1 Ghz or higher
- RAM – 1 GB or more
- Hard Drive – ATA-100 or SCSI with 100 MB free space or more
- Network interface card (two may be needed depending on your chosen network configuration)
- Windows 2003 server or Windows 2008 server
- Microsoft Internet Information Services (IIS) 6.0 with a Windows 2003 server or Microsoft Internet Information Services (IIS) 7.5 with a Windows 2008 server
- CD-ROM drive
- Access to a new or existing network installation of AD Summation iBlaze3.1 on a Windows 2003 or 2008 server on the same LAN as the WebBlaze server
- WebBlaze server must be a member server in the same domain as the AD Summation LAN server OR two local service accounts must be created (one service account on the WebBlaze server and another identical account on the AD Summation LAN server)
- Network connectivity between the AD Summation WebBlaze server and the AD Summation LAN server containing a network case (typically on the LAN)
- Network connection accessible to client computers (typically a live Internet IP address)
- Microsoft Internet Explorer 7.x – 8.x
- Microsoft .NET Framework 2.0 with Windows 2003 server or Microsoft .NET Framework 3.5 with Windows 2008 Server
- Windows Installer 3.1
- MDAC 2.7 or later (installed automatically, if necessary)

WEBBLAZE CLIENT RECOMMENDED SPECIFICATIONS

- Microsoft Internet Explorer 7.x - 8.x , set to allow session cookies and active scripting
- Network connectivity to server (typically over the Internet or the LAN)
- Microsoft Internet Explorer security set to allow ActiveX controls to install and run

PREREQUISITE CHECKLIST

- Verify that your Web server is running IIS and ASP.NET
- Ensure that all security precautions have been taken (firewall, network configuration, OS patches, Microsoft IIS lockdown tool applied, and so on)

- Connect the server to appropriate networks (decide network topology)
- Set up the DNS entry to be used by the clients to connect to the AD Summation WebBlaze server
- Install the SSL certificate
- Create a service account for AD Summation WebBlaze
- Install AD Summation WebBlaze

Installing AD Summation WebBlaze

This section discusses the procedures for installing AD Summation WebBlaze. For information about upgrading an existing AD Summation WebBlaze installation, see Upgrading AD Summation WebBlaze.

AD Summation WebBlaze is useful for remote or traveling employees who have Internet access, people outside of your firm with whom you need to share information (such as expert witnesses or co-counsel), or novice users who would benefit from a simplified user interface.

AD Summation has true *hyper-concurrent licensing*, which means that the AD Summation iBlaze network client installations, mobile installations and the AD Summation WebBlaze installation all share a pool of licenses that is dynamically allocated between Web and console clients.

As a best practice, it is recommended that you install AD Summation WebBlaze on a separate physical server from your database server. If you choose to install WebBlaze on the same server as your SQL Server, and your server hardware configuration is inadequate, you may experience lags in performance in both console and Web clients.

NETWORK TOPOLOGY CONSIDERATIONS

The first step in the installation process is to determine which network topology is appropriate for your environment.

Two questions need to be answered at this point:

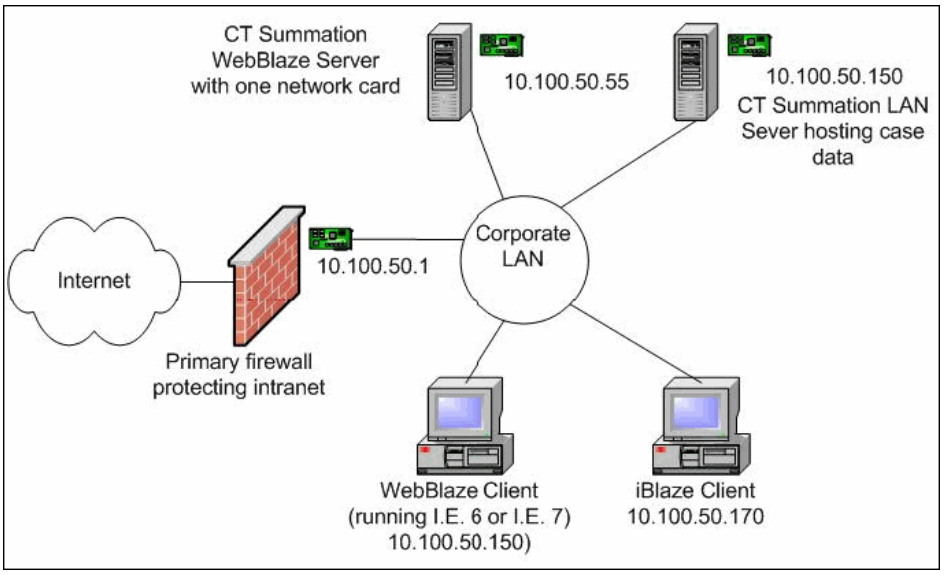
- How will the WebBlaze clients access the AD Summation WebBlaze server (for example, over the Internet or over an intranet)?
  - If the server will be accessed over the Internet, consider using Options 2, 3, or 4.
  - If the server will be accessed over an intranet, or if users will connect over a VPN, consider using Option 1.
- What type of network security architecture is in place on the network?
  - If your security policies do not allow for servers to be connected to both the network and the Internet, consider Options 1 or 3.
  - If your security policies do allow for servers to be connected to both the network and the Internet AND users need access over the Internet, consider Options 2, 3, or 4.

All network and system security precautions should be followed in accordance with sound security practices based on the chosen network topology. Four potential network topologies are described on the following pages. These diagrams may be helpful in determining the appropriate topology to use in your environment.

NOTE: Other topologies are certainly possible. The basic requirement is that the AD Summation WebBlaze server is able to connect to the case data stored on your network location (using Microsoft networking) AND that it has an address that is available to the clients that will need access (that are connected to the Internet or intranet).

OPTION 1: INTRANET ACCESS ONLY

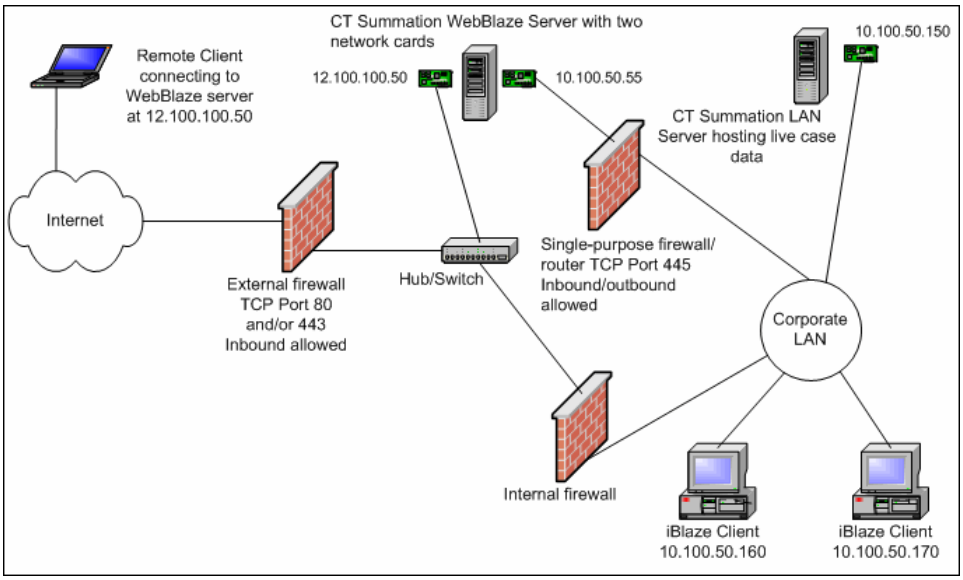
Option 1 illustrates an environment where the AD Summation WebBlaze server is available only to those workstations that are connected to the firm's network. In this configuration, access is only available to those with access to the firm's trusted internal network. The connection to the intranet may be through the network, through a dedicated point-to-point WAN connection (such as a T-1 connection), or a Virtual Private Network (VPN). This configuration is considered to be the most secure because it is only available to those with physical and/or virtual access to the internal network. However, remote users will require more than a simple Internet connection (for example, a VPN connection over the Internet) in order to access the WebBlaze server. In this configuration, the WebBlaze server may also act as the AD Summation server.



Intranet Access Only

OPTION 2: INTERNET ACCESSIBLE, MOST SECURE INTERNET-AVAILABLE CONFIGURATION

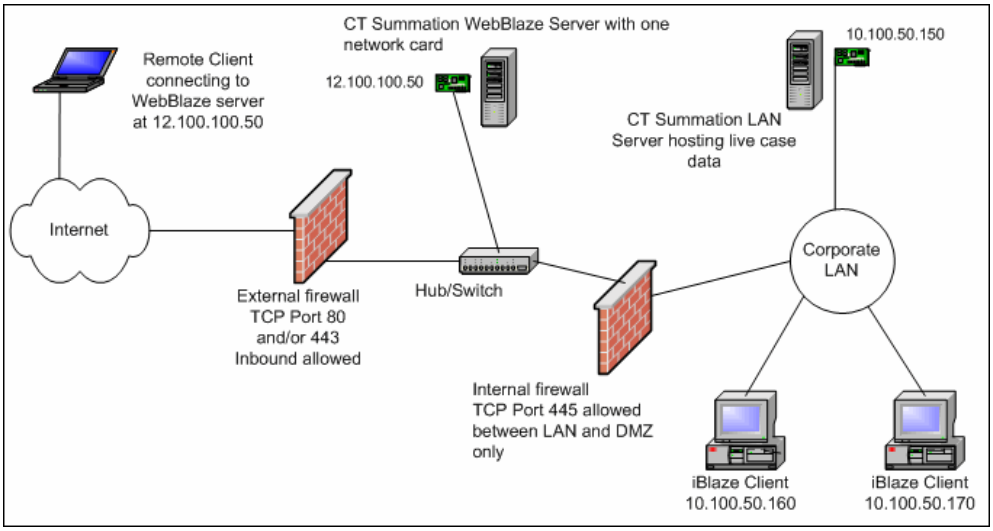
Option 2 illustrates an environment where the AD Summation WebBlaze server is available to users who are connected over the Internet. In this environment, users need a connection to the Internet and must know the DNS address or the IP address of the WebBlaze server (in this example, 12.100.100.50). This configuration is considered to be the most secure Internet-accessible architecture. This is because the WebBlaze server is located in the network DMZ and multiple layers of network security are in place to protect the "internal" network. However, this configuration is the most complex and costly due to the addition of a firewall designed to isolate the server's "inside" address from the network.



Internet Accessible, Most Secure Internet-Available Configuration

OPTION 3: INTERNET ACCESSIBLE WITH THE LOWEST COST

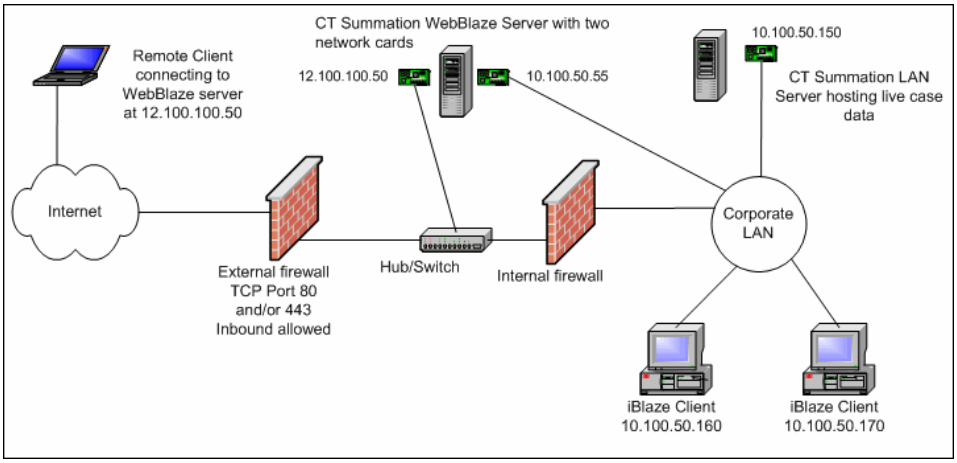
Option 3 illustrates an environment where the AD Summation WebBlaze server is available to users who are connected over the Internet. In this environment, users need a connection to the Internet and must know the DNS address or the IP address of the WebBlaze server (in this example, 12.100.100.50). This configuration is considered to be the most secure configuration after Option 2. This is because the WebBlaze server is located in the network DMZ and has no direct connection to the internal network. However, this configuration MAY require additional configuration of the “internal firewall” in order to allow the WebBlaze server to connect to the AD Summation case data server.



Internet Accessible with the Lowest Cost

OPTION 4: INTERNET ACCESSIBLE, SIMPLEST INTERNET-AVAILABLE CONFIGURATION

Option 4 illustrates an environment where the AD Summation WebBlaze server is available to users connected over the Internet. Users wanting to connect to the WebBlaze server in this environment need a connection to the Internet and need to know the DNS address or the IP address of the WebBlaze server (in this example, 12.100.100.50). This configuration is considered to be the simplest Internet-accessible configuration because the WebBlaze server handles the connections to both the Internet and the corporate network.



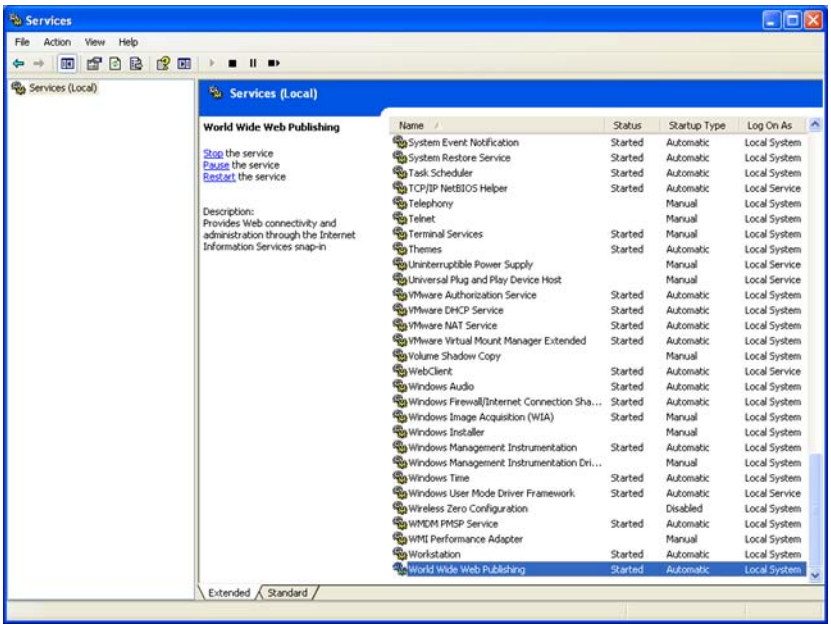
Internet Accessible, Simplest Internet-Available Configuration

IIS SERVICE SETUP

Prior to connecting the Web server to your network, you should verify that it is configured to run IIS and that it has been secured.

To verify that the Web server has IIS running:

1. Go to the **Administrative Tools** folder in the **Control Panel** on the Web server, and double-click **Services** to run the **Windows Services Manager**.
2. Scroll to the bottom and check to see if the **World Wide Web Publishing** service is running (the status should say **Started**).



World Wide Web Publishing Service

3. If you have the service installed but the status is not **Started**, double-click the **World Wide Web Publishing** service, click **Start**, and set it to **Automatic**.
4. If you do not see an entry for **World Wide Web Publishing** service, you do not have IIS installed. To install IIS you will need your Windows Server CD. IIS is a windows component that you can add from the CD.
5. To add IIS to your Windows server, go to your **Control Panel**, click **Add/Remove Programs**, and on the left panel, click **Add/Remove Windows Components**. In Windows 2003 Server, you will have to add the **Application Server** component.
6. While adding IIS in Windows 2003 Server, make sure to select the ASP.NET sub-selection.

WEB SERVER SECURITY CONSIDERATIONS

AD Summation recommends that you take the following network security steps prior to connecting the server to any “un-trusted” network (particularly the Internet). You may choose to implement steps above and beyond these in order to secure your server as appropriate for your network.

1. For any external facing AD Summation WebBlaze server, place the server behind an appropriately configured firewall. Connecting any server directly to the Internet without a firewall is not advisable under any circumstances.
2. For an external facing web server, configure the server hardware so that it has separate external and internal facing network interface cards (NICs).
3. Microsoft Networking and NetBIOS should be disabled on the network interface card that is exposed to the Internet. For your external firewall, the only ports that should be allowed are ports 80 and 443 (HTTP and HTTPS).
4. For your internal facing NIC and firewall, you will need to have Microsoft Networking and NetBIOS enabled. In addition, the internal firewall will need to allow Microsoft Networking and File access ports (Ports 135-

139 and Port 445) and the SQL Server access port (Port 1433 by default unless overridden on the SQL Server).

5. Apply the latest anti-virus program updates and pattern files. Make sure to configure the server to automatically download the latest pattern files automatically.
6. Apply the latest Microsoft Windows Updates and Service Packs. The server should be regularly checked for the latest updates and patches or optionally configured to download the Windows Update patches automatically.
7. For Windows 2003 servers with SP1, run the Security Configuration Wizard that is part of SP1 and lock down all non-essential services running on the web server and restrict the ports allowed by the built in Windows Firewall.

SETTING UP A DNS ENTRY

If you want to make the server available to your clients with a DNS address (such as *https://WebBlaze.YourDomain.com*), contact your DNS provider to set up an **A record** pointing to the server IP address that clients will use to connect.

NOTE: If you do not want to use a DNS entry, you can use the IP address instead. For example if your server's IP address is *12.100.100.50*, you can connect to *http://12.100.100.50/webblaze*.

INSTALLING AN SSL CERTIFICATE

If you want to encrypt your data in transit as it traverses the Internet for security reasons, a secure sockets layer (SSL) certificate must be installed.

AD Summation highly recommends the use of an SSL certificate in conjunction with the AD Summation WebBlaze installation. Contact your AD Summation sales representative at (800) 735-7866 for details. Note that the SSL certificate is provided by a third-party and the process of obtaining a certificate can take up to three days (however, it will typically take less than 24 hours) so plan accordingly.

CONFIGURING A WEBBLAZE SERVICE ACCOUNT

The AD Summation WebBlaze application requires the creation of a domain user account that will be used by WebBlaze to access the case data on the AD Summation iBlaze server. You have two options for setting up the **WBService** account: *synchronized accounts* or *domain membership*. These methods are explained below. Under most circumstances, using synchronized accounts is the best option for security reasons; however, if you are using AD Summation WebBlaze as an intranet server (Option 1), the domain membership method is the simplest.

To use the synchronized accounts method:

1. Create a **local** user account on the AD Summation WebBlaze server (typically done from the Microsoft Windows **User Manager** in the **Computer Management** console) named **WBService** and assign a complex password.

   NOTE: Any valid NT user name can be created, however, to keep things simple, this document refers to WBService.

2. Create a **local** user account on the AD Summation iBlaze server named **WBService** and assign a complex password that matches the password created in Step 1 above. If you are storing images or other case components on yet another server, repeat this step for each of the additional file servers.

3. Give the **WBService** account permissions to access the AD Summation case data (such as the summary database, transcripts, and images) on the AD Summation iBlaze server and any other servers included in Step 2 above. This is done from the **Security** tab in the folder properties on the individual data servers. Be sure to give the **WBService** account both file-system permissions AND share-level permissions.

To use the domain membership method:

1. Create a user account on the domain (typically done through the Microsoft Windows **Active Directory Users and Computers Console** or **User Manager for Domains**) named **WBService** and assign a complex password.

   NOTE: Any valid NT user name can be created, however, to keep things simple, this document refers to **WBService**.

2. Give the **WBService** account permissions to access the AD Summation case data (transcripts, electronic documents, and images). This is done from the **Security** tab in the folder properties on the case data server. Be sure to give the **WBService** account both file-system permissions AND share-level permissions. Do not give the **WBService** account direct rights in **iBlaze Manager** on the SQL Server. Instead assign a SQL Server user for each AD Summation WebBlaze group that you create in the AD Summation iBlaze **Administrator Console**.

   NOTE: If you are using NT-integrated security in AD Summation iBlaze, make sure to add **WBService** to the **SWUsers** group on your AD Summation iBlaze server.

AD SUMMATION WEBBLAZE INSTALLATION

Once you have determined your topology and have completed the pre-installation steps, you can begin the actual AD Summation WebBlaze product installation. At this point, you must have already completed all of the steps in the previous section, and connected the server to the appropriate network(s).

NOTE: You may be prompted to reboot the server at the end of the following installation process. Plan accordingly.

The .NET framework is a Windows component that is not installed by default on Windows 2003 server. If you are planning to install AD Summation WebBlaze on a Windows 2003 server, you must first install the .NET framework by following these steps:

1. Double-click the **Add/Remove Programs** in the **Control Panel**.
2. Choose **Add/Remove Windows Components**.
3. Highlight **Application Server** and click **Details**.
4. Click the check box next to **ASP.NET**.
5. Click **OK** and **Next** to save these changes.

Prior to installing AD Summation WebBlaze, you will need to gather the following information:

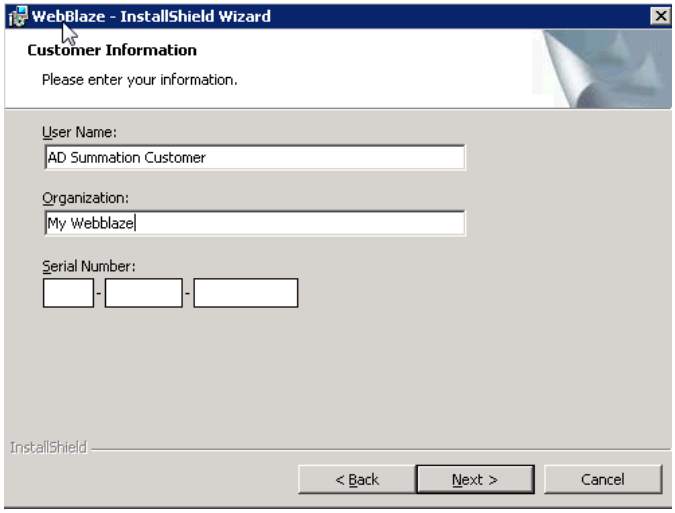
- **Case Data Location** – Note the location of your AD Summation iBlaze network cases. This shared network directory must be accessible to the AD Summation WebBlaze server using Microsoft Networking. A UNC path is required; **DO NOT** use a mapped drive. In addition you should verify that your Web server has network access to your SQL Server (default TCP SQL Server port is 1433 but this may be changed by the database administrator).

- WebBlaze account **username** and **password**.

To install AD Summation WebBlaze:

1. Begin the AD Summation WebBlaze installation from the installation CD by running **WebBlazeSetup.exe**. DO NOT run the **Summation WebBlaze.msi** file directly.

   The **WebBlazeSetup.exe** program performs prerequisite testing and installation as needed. Depending on the currently installed server components (such as MDAC, MSXML, and so on), the setup will check for and install the appropriate software prerequisites. You may be prompted to install the individual server components; if so, answer affirmatively to allow the setup to continue and click **Next >**.
   The **Customer Information** dialog box is displayed.



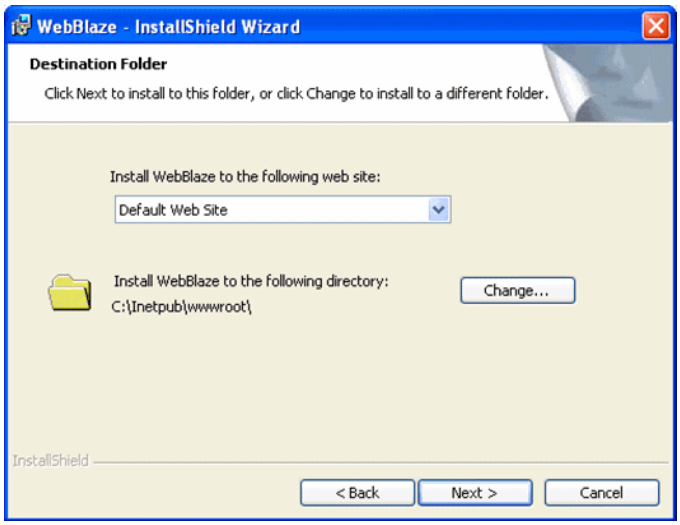
Customer Information Dialog Box

2. Enter your customer information, check the box in the lower left corner to link AD Summation WebBlaze to a AD Summation iBlaze network share, and click **Next >**.
   The **License Agreement** dialog box is displayed.

3. Accept the terms of the license agreement, then click **Next >**.
   The **AD Summation iBlaze Location** dialog box is displayed.

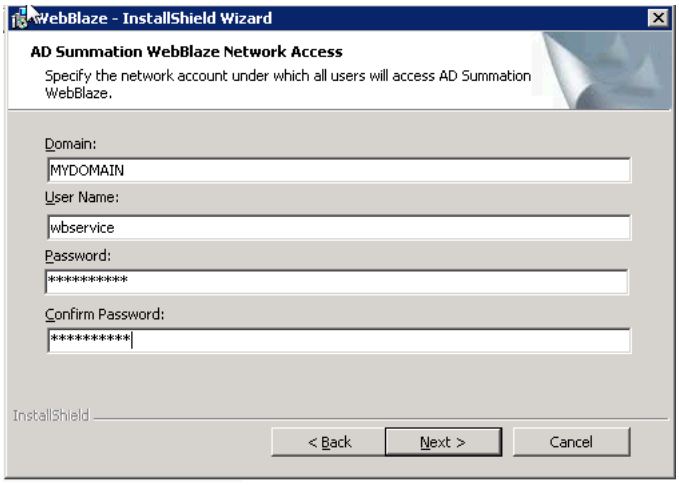
4. Enter the UNC path or browse to the case data directory on the network. This location should be the root of the AD Summation application directory (the *application directory* is the directory containing the **SummSSE.exe** file). If the AD Summation WebBlaze server also acts as the AD Summation iBlaze server, you must use the UNC path (for example, *\\WBServername\Share\iBlaze*) to the data, NOT the local hard drive (for example, *C:\Share\iBlaze*). This entry MUST be a UNC path, and must NOT be a mapped drive.

5. Click **Next >**.
   The **Destination Folder** dialog box is displayed, giving you the option to change the displayed local disk location of the WebBlaze server program.



Destination Folder Dialog Box

6. It is recommended that you accept the default path that is displayed (for example, *C:\Inetpub\wwwroot*). If you have multiple web site repositories setup on the local IIS server, you can select the Default or a custom one from the drop down menu. Click **Next >** to install to the selected location.
   The **AD Summation WebBlaze Network Access** dialog box is displayed.

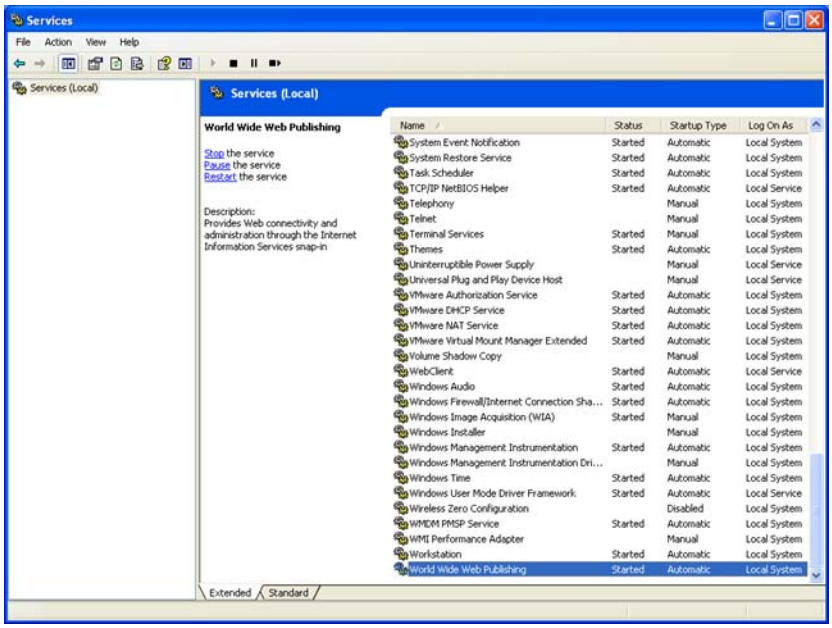


AD Summation WebBlaze Network Access Dialog Box

7. Complete the information on the dialog box:
   - **Domain** – If you chose the synchronized accounts method, enter the name of the AD Summation WebBlaze server. If you chose the domain membership method, enter the name of the Windows NT domain of which the AD Summation case data server is a member.
   - **User Name** – Type the NT local or domain account created in the section Configuring a WebBlaze Service Account. Typically the user name is **WBService**.
   - **Password** – Type the password for the local or domain account specified above. Re-type this password in the **Confirm Password** box.
8. Click **Next >**.
   The **Specify Advanced Settings used by AD Summation WebBlaze** dialog box is displayed.

9. Select the options necessary on the dialog box:
   - **Access AD Summation WebBlaze Using** – Specify whether an SSL certificate has been installed to encrypt network traffic between the AD Summation WebBlaze server and the client. If you have not yet installed an SSL certificate for this web server, you MUST select **HTTP**. (If you choose **HTTPS**, and an SSL certificate is not installed, AD Summation WebBlaze will not function properly. Choose **HTTPS** only if you have already successfully installed an SSL certificate on this server).
   - **Transformation Server** –Specify a port number for the transformation server in the available field. This port will be used for delivery of the Near Native eDoc mode to WebBlaze clients. It is recommended that a port in the "dynamic range"(ports 49152 through 65535) is specified. You may need to open the TCP port you specify on your firewall to allow for Near Native viewing.
   - **Make AD Summation WebBlaze the default application on this IIS server** – Select this option to direct all users of the AD Summation WebBlaze application by default. **Do not select this option if you are hosting other applications on this server**. (If you select this option, users connect directly to the server and are directed to the WebBlaze logon page (for example, *https://WebBlaze.mydomain.com*). If you do NOT select this option, users must select the WebBlaze sub-directory when accessing WebBlaze on the server (for example, *https://WebBlaze.mydomain.com/WebBlaze*).

10. Once you have entered the information, click **Next >**.
11. Click **Install** to begin the installation.
12. When the installation is complete, the **InstallShield Wizard Completed** dialog box is displayed. If you leave the check box selected and click **Finish**, the installer will proceed to install the Help files.
13. Depending upon the files installed by the setup program, the **AD Summation WebBlaze Installer Information** dialog box may be displayed. If the dialog box is displayed, click **No** for now.
14. Click **Finish** when prompted that the installation is complete.
15. You may be prompted to reboot your server or restart IIS. To restart IIS, go to Start->Run->type ***iisreset*** and select **OK**, or access the Microsoft Windows **Services** applet and restart the **World Wide Web Publishing** service. This step is required to ensure proper operation of your AD Summation WebBlaze server.



World Wide Web Publishing Service

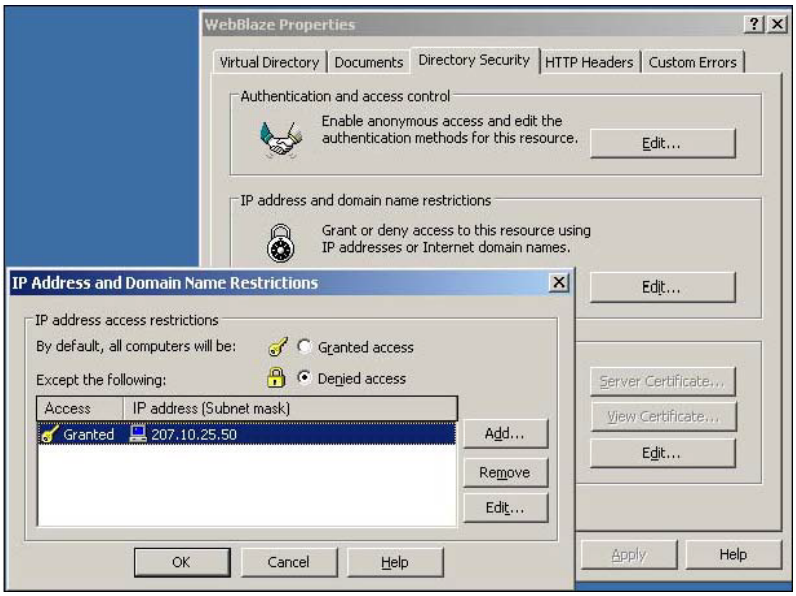
SECURING AD SUMMATION WEBBLAZE

AD Summation highly recommends that you use the following tips to ensure the most secure environment possible for your AD Summation WebBlaze server. Note that many of these tips are included in the main body of this guide as well. This list is intended as an additional summary resource focused only on security.

NOTE: You are responsible for the security of your AD Summation WebBlaze server. These tips are intended as a general guide. You may choose to perform additional steps to increase the security of your WebBlaze server depending on your environment.

Security Tips:

- **Install and use an SSL certificate** – Encrypt data that will be traversing the Internet. AD Summation provides a complimentary SSL certificate from **InstantSSL** that is good for twelve months. Contact your account manager.
  For detailed instructions on generating an SSL request and installing the SSL certificate, refer to the subsequent section on SSL Certificates in this section.
- **Choose a complex password** – Choose a complex password for the **WBService** account. A good password should have eight or more characters, at least one number, at least one special character, and should not contain a word or name.
- **Limit access to case data** – When establishing permissions in the **Administrator Console**, make sure to limit users to groups that have an appropriate level of permissions on a specific set of cases.
- **Limit server access to specific IP address(es)** – If you know the IP address(es) of those who should have access to the server, you can set these addresses in the IIS server management tool in the **IP address and domain name restrictions area** on the **Directory Security** tab.



Specifying IP Address(es)

- **Use a properly configured network firewall** – If the server will be available on an un-trusted network (such as the Internet), never place any server directly on that network. Always use a firewall to protect the server. You should allow only port 80 and/or port 443 on the firewall protecting the server from the Internet.
- **Disable any unnecessary services on the WebBlaze server** – Disable any services that are not necessary, for example, WINS, Microsoft networking (on the "outside" network adapter), SNMP, DHCP, and so on.
- **Set the lockout interval for failed login attempts** – Use the **Administrator's Tools** in the AD Summation WebBlaze user interface to administer the **Login Status** and set the lockout interval as appropriate (the default is five minutes). This will lock out accounts in case of brute force password attacks. For more information, see the Help in AD Summation WebBlaze.
- **Lock down the WBService account** – The following steps are recommended to lock down the **WBService** account:
  - If you are using the synchronized accounts method, make the **WBService** account a member of the **Guests** group and remove it from the **Users** group on both the WebBlaze and AD Summation iBlaze server. If you are using the domain membership method, add the **WBService** account to the **Domain Guests** account and remove it from the **Domain Users** group.
  - Give the **WBService** account permissions ONLY to the AD Summation data share on the AD Summation iBlaze server. Do not give this account access to any other directories on your network.
  - Set up auditing on the AD Summation iBlaze server and the AD Summation WebBlaze server to audit the activities of the **WBService** account.
- Set complex password rules for AD Summation WebBlaze accounts – In the **Administrator Console**, on the **ULM** tab, click **WebBlaze Password Rules**. Set the minimum password length to a number between six and twenty. Click **Yes** under the **Require Complex Password** option.

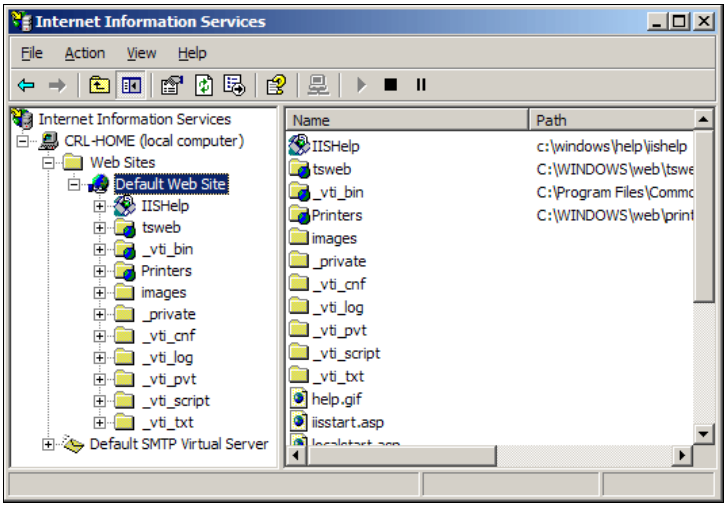
GENERATING AN IIS SSL CERTIFICATE REQUEST

Prior to generating an SSL certificate, you should know the DNS entry you want to create for this certificate (for example, *webblaze.mydomain.com*) and confirm that the domain is available and registered with your DNS provider.

The first step to installing an SSL certificate on your Web server is to generate a Certificate Signing Request (CSR). A CSR is a file containing your IIS SSL certificate application information, including your Public Key. Your CSR is required during the enrollment process.

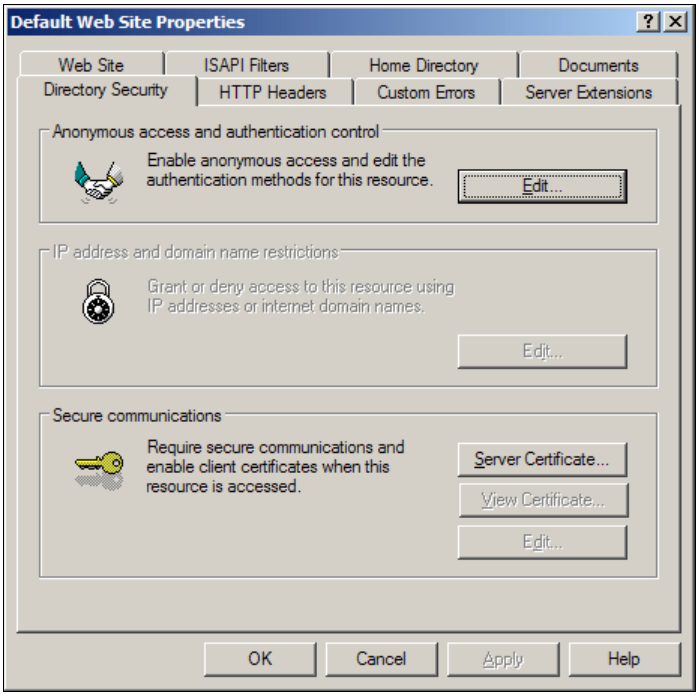
To generate a CSR:

1. Select **Administrative Tools** from your **Control Panel**.
2. Select **Internet Information Services Manager**.
   The **Internet Information Services** window is displayed.



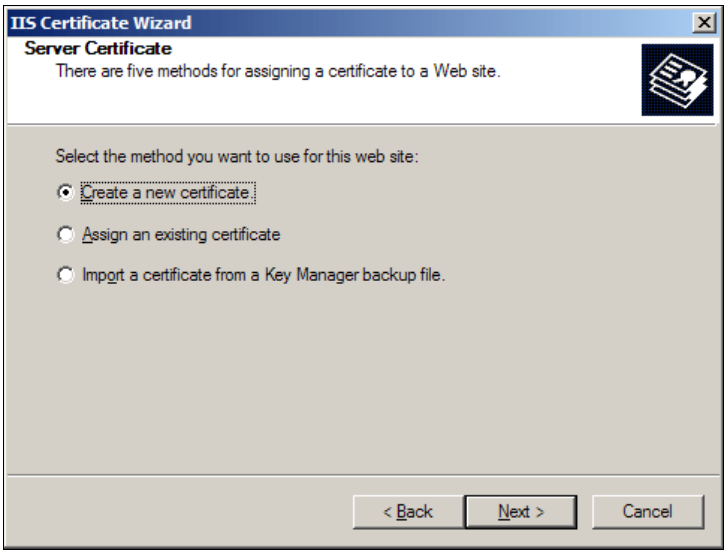
Internet Information Services Window

3. Right-click **Default Web Site**, select **Properties** from the menu, and then click the **Directory Security** tab.
   The **Directory Security** tab is displayed.



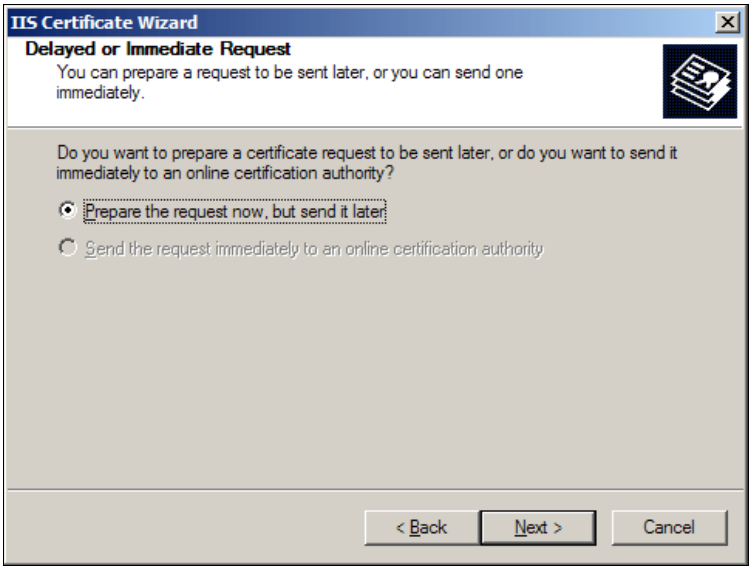
Directory Security Tab

4. Click **Server Certificate….**
   The **IIS Certificate Wizard** is launched.



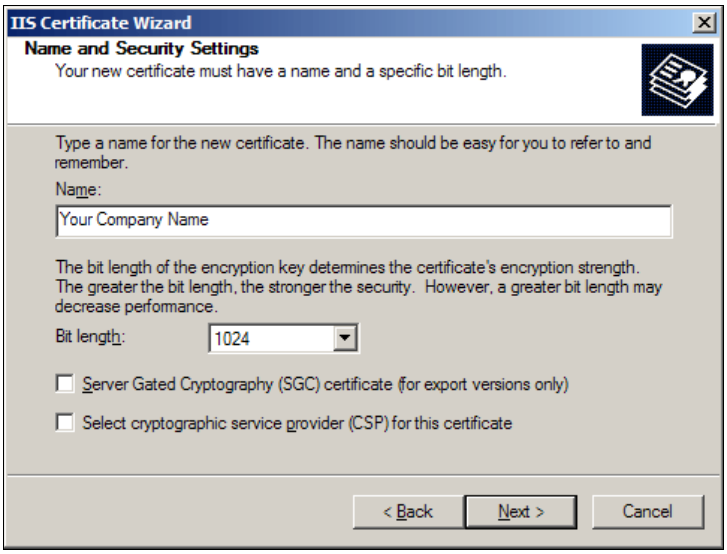
Server Certificate Dialog Box

5. Select **Create a new certificate**, and then click **Next >**.
   The **Delayed or Immediate Request** dialog box is displayed.



Delayed or Immediate Request Dialog Box

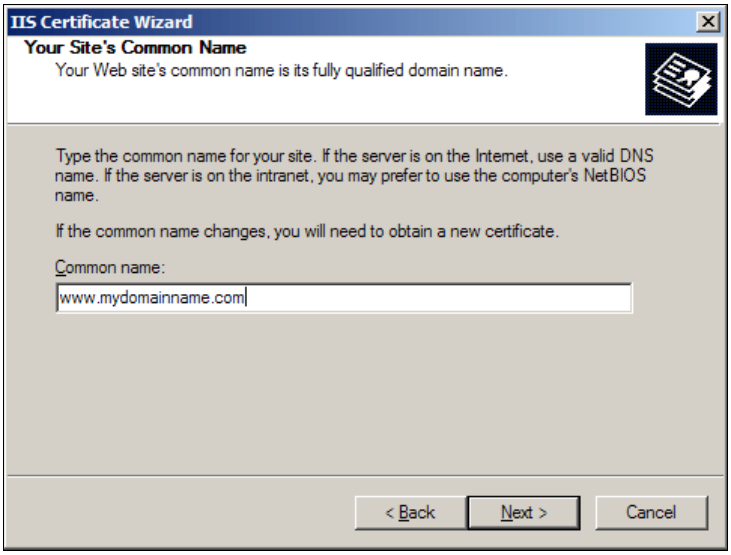
6. Select **Prepare the request now, but send it later**, and then click **Next >**.
   The **Name and Security Settings** dialog box is displayed.



Name and Security Settings

7. Provide a **Name** for the certificate. (This is for your records only and should be easily identifiable). Select the desired **Bit length** for the SSL key. If your server is 40 bit enabled, you will generate a 512 bit key. If your server is 128 bit, you can generate keys of up to 1024 bits. Once you select the bit length, click **Next >**.

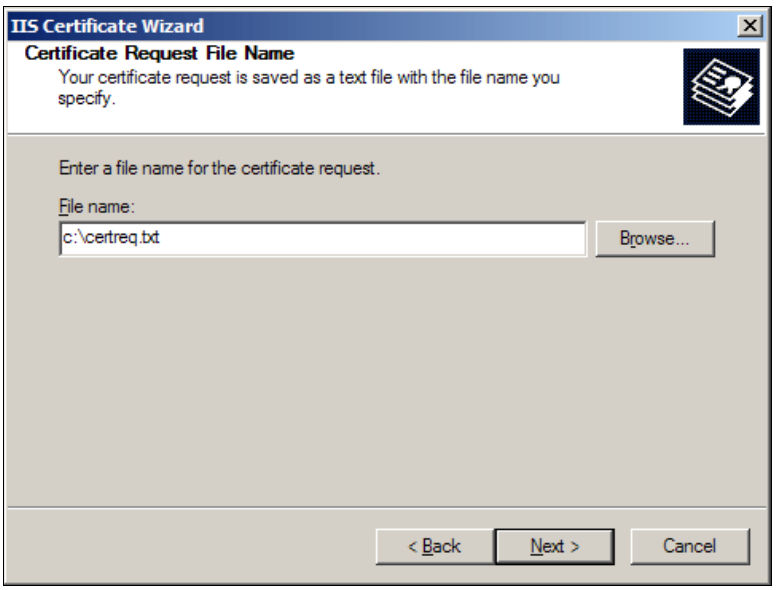
8. Complete the **Organization** and **Organization Unit** boxes with your company name and department respectively, and then click **Next >**.
   The **Your Site's Common Name** dialog box is displayed.



Your Site's Common Name Dialog Box

9. Complete the **Common Name** field with the fully qualified domain name (FQDN) or the Web address for which you plan to use your IIS SSL Certificate (in other words, the area of your site that users will to connect to using SSL). This should be the same name you registered with your DNS provider. For example, if you want your AD Summation WebBlaze server to be available at the secure address *https://webblaze.mydomain.com*, you must register this address as an **A type** address with your DNS provider, and enter **webblaze.mydomain.com** as the **Common name**, and then click **Next >**.

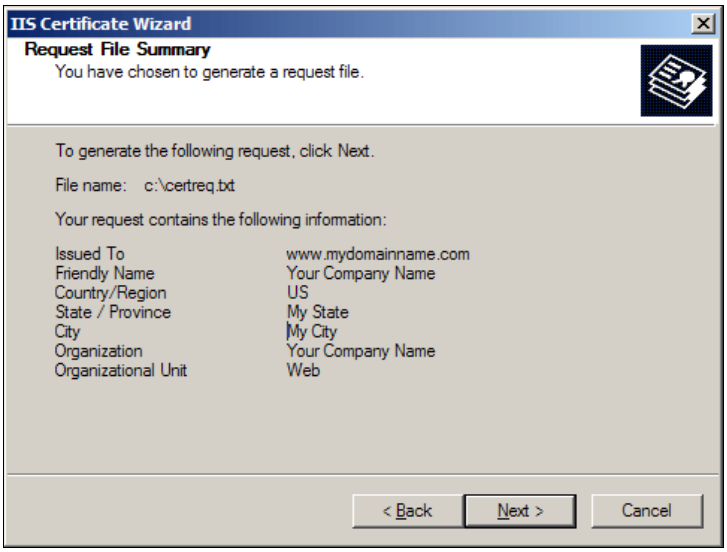
10. Enter your **Country**, **State**, and **City**. Click **Next >**.
    The **Certificate Request File Name** dialog box is displayed.



Certificate Request File Name

11. In the **File name** box, enter the location and file name where you want to save your CSR. You will need this CSR to enroll for your IIS SSL Certificate.

12. Click **Next >**.
    The **Request File Summary** dialog box is displayed.



Request File Summary Dialog Box

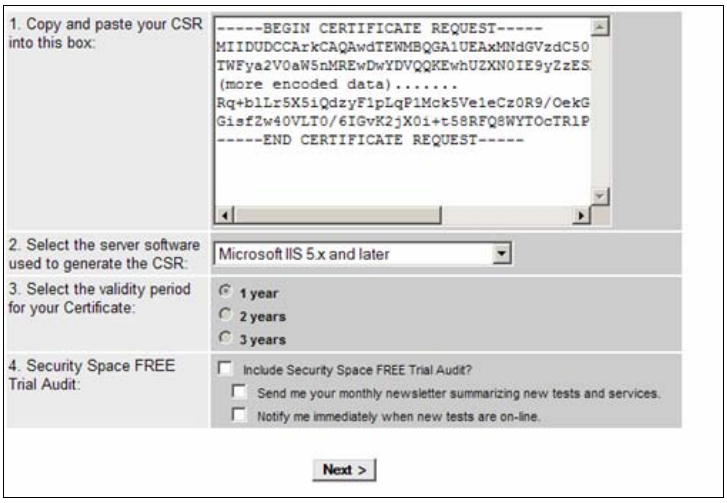
13. Verify the details you have entered paying special attention to the **Issued To** portion to verify that the domain is correct. Once you are certain that the details are absolutely correct, click **Next >**.

14. At this point, you must save your private key:

    - On the desktop, click **Start**, select **Run**, type **mmc** and click **OK**.
      An MMC **Console** window is displayed.
    - From the **File** menu, select **Add/Remove Snap-in**.
      The **Add/Remove Snap-in** dialog box is displayed.
    - Click **Add**.
      The **Add Standalone Snap-in** dialog box is displayed.
    - Select **Certificates** from the **Snap-ins** list and click **Add**.
      The **Certificates Snap-in** dialog box is displayed.
    - Select **Computer Account** and click **Next >**.
      The **Select Computer** dialog box is displayed.
    - Select **Local Computer** and click **Finish**.
    - Close the **Add Standalone Snap-in** dialog box.
    - On the **Add/Remove Snap-in** dialog box, click **OK**.
    - On the **MMC Console** window, right-click **Requests** and select **All Tasks** and **Export** from the menu.
    - Save the text file.

    NOTE: Make a note of your password and backup your key, as these are known only to you.

- When you make your application on the web site, make sure you add the CSR in its entirety into the appropriate section of the enrollment form – including the following line, and click **Next >**.



Certificate Request Application

- Confirm your details in the enrollment form and click **Next >**.
  An e-mail message will be sent to you confirming your request.

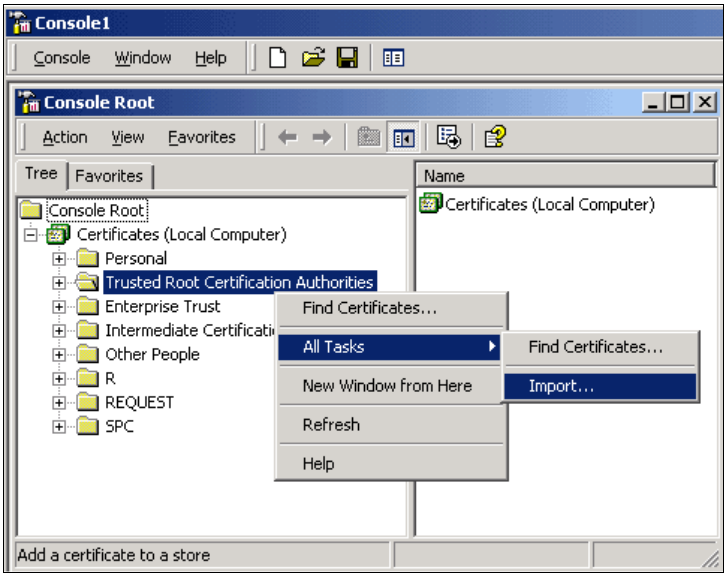
INSTALLING YOUR IIS SSL CERTIFICATE ON MICROSOFT IIS 5.X/6.X

You will receive three certificates from InstantSSL. Save these certificates to the desktop of the Web server computer, and complete the following steps:

1. On the desktop, click **Start**, select **Run**, type **mmc** and click **OK**.
   An **MMC Console** window is displayed.
2. From the **File** menu, select **Add/Remove Snap in**.
   The **Add/Remove Snap in** dialog box is displayed.
3. Click **Add**.
   The **Add Standalone Snap-in** dialog box is displayed.
4. Select **Certificates** from **Snap-ins** list and click **Add**.
   The **Certificates Snap-in** dialog box is displayed.
5. Select **Computer Account** and click **Next**.
   The **Select Computer** dialog box is displayed.
6. Select **Local Computer** and click **Finish**.
7. Close the **Add Standalone Snap-in** dialog box.
8. On the **Add/Remove Snap-in** dialog box, click **OK**.
9. Return to the MMC **Console** window.

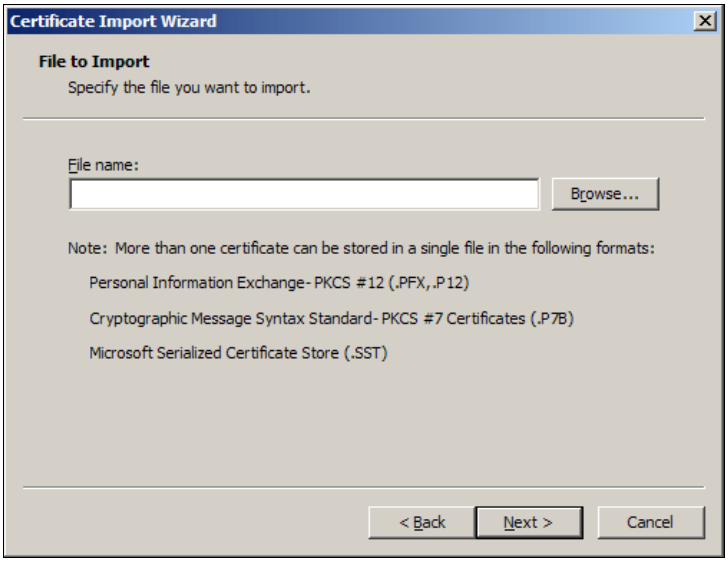
To install the **GTECyberTrustRoot** certificate:

1. On the MMC **Console,** right-click the **Trusted Root Certification Authorities**, and from the menu select **All Tasks** and **Import**.



Importing Certificate

2. Click **Next >**.
   The **File to Import** dialog box is displayed.



File to Import Dialog Box

3. Browse to and select the **GTECyberTrustRoot** certificate, and then click **Next >**.
4. When the wizard is complete, click **Finish**.

To install the **ComodoSecurityServicesCA Certificate**:

1. From the **Control Panel**, double-click **Administrative Tools** and start **Internet Information Services Manager**.
2. Right-click **Default Web Site**, and then select **Properties**.
3. On the **Default Web Site Properties** dialog box, click the **Directory Security** tab.
4. Click **Server Certificate**.
5. Select **Process Pending Request and install the certificate**, and then click **Next >**.
6. Browse to and locate your IIS SSL certificate, and click **Next >**.
7. Review the summary screen to make sure that you are processing the correct certificate, and then click **Next >**.
   A confirmation dialog box is displayed.
8. Review the information, and click **Next >**.
   The IIS SSL server certificate is installed.
9. Reboot to complete the process.

Upgrading AD Summation WebBlaze

This section discusses the procedures for upgrading to the latest version of AD Summation WebBlaze. For information about performing a new installation, see Installing AD Summation WebBlaze.

If you are currently working in an earlier version of AD Summation WebBlaze, use the following instructions to upgrade to version 3.1. You may need to reboot the server at the end of the upgrade process, so plan accordingly. Note that in WebBlaze Version 3.1, Microsoft .NET Framework 2.0 is required. If this application is not already installed on your WebBlaze server, you will have to install it during the upgrade process.

To upgrade AD Summation WebBlaze:

1. Go to the WebBlaze server and begin the WebBlaze upgrade from the installation CD by running **WebBlazeSetup.exe**. Do NOT run the **WebBlaze.msi** file directly.
2. Microsoft .NET Framework 2.0 must be installed on the WebBlaze server before you can upgrade to WebBlaze 3.1.
   - If .NET Framework 2.0 is not already installed, a message is displayed asking if you would like to install it. Proceed to Step 3.
   - If .NET Framework 2.0 is already installed, the **Welcome to the InstallShield Wizard for WebBlaze** dialog box is displayed. Proceed to Step 9.
3. Click **Yes**.
   The **Welcome to Microsoft .NET Framework 2.0 Setup** dialog box is displayed.
4. Click **Next >**.
   The **End-User License Agreement** screen is displayed.
5. Read and accept the Microsoft .NET Framework license agreement, and click **Install**.
6. The **Installing Components** and the **Preparing to Install** dialog boxes are displayed as Microsoft .NET Framework 2.0 is installed.
7. When the installation is complete, the **Setup Complete** dialog box is displayed.
   Click **Finish**.
8. The **Welcome to the InstallShield Wizard for WebBlaze** dialog box is displayed.
9. Click **Next >**.
   The **Customer Information** dialog box is displayed with the information filled out for you.
10. Click **Next >**.
    The **License Agreement** dialog box is displayed.
11. Read and accept the license agreement, and click **Next >**.
    The **AD Summation iBlaze Location** dialog box is displayed, with the network location filled out for you.

12. Click **Next >**.
    The **Destination Folder** dialog box is displayed with the information filled out for you.
13. Click **Next >**.
    The **AD Summation WebBlaze Network Access** dialog box is displayed with the information filled out for you.
14. Click **Next >**.
    The **Specify Advanced Settings used by AD Summation WebBlaze** dialog box is displayed.
15. Click **Next >**.
    A dialog box is displayed, informing you that the wizard is ready to begin the installation.
16. Click **Install**.
    The upgrade begins. When the upgrade is complete, the **InstallShield Wizard Completed** dialog box is displayed.
17. If you want to install the WebBlaze Help files, select the **Yes, launch Help file installation now** check box. Click **Finish**.
    The WebBlaze Help is installed.
18. Click **Finish** again.
    A final message is displayed, informing you that you should restart IIS and/or restart the WebBlaze server. Click **OK**.

    NOTE: Depending upon the files installed during the upgrade, the **AD Summation WebBlaze Installer Information** dialog box may be displayed. If this dialog box is displayed, click **No** for now. After completing the upgrade process, reboot your server.
19. Access **Internet Information Services** and right-click the WebBlaze server name, select **All Tasks**, and select **Restart IIS** from the sub-menu.
    Restarting IIS is required to ensure proper operation of your WebBlaze server.