



Installing and Configuring Blade File Transfer System Server

Please use this guide to install, configure and secure your Blade File Transfer System Server on Windows Server 2003 and Windows Server 2008.

Tip: Once you have installed the software, you can always access this guide from your Blade Server. It can be found under **Start | Programs | Blade | Blade File Transfer System Server | Configuration Guide**.

In this Document

In this Document	1
Blade Server Pre-Requisites	2
Network Pre-Requisites	2
Installing the Blade Server	2
Configure IIS – Windows Server 2003	3
Configure IIS – Windows Server 2008	4
Configure Authentication - Windows Server 2003	4
Configure Blade Server Settings	5
Configure Secure Sockets Layer (SSL) – Windows Server 2003	8
Configure Secure Sockets Layer (SSL) – Windows Server 2008	9
Test File Upload and Download using WebClient.....	9
Known Issue – Symantec Anti Virus software	11
Informational Appendix A: File Security and Permissions.....	12
Running the Blade Server with Basic Authentication	12
Running the Blade Server with Anonymous Authentication	12
Support and Troubleshooting	12
Informational Appendix B: Virtual Directory Security Settings.....	12
Informational Appendix C: Installing IIS and ASP.NET on Windows Server 2003	13
Informational Appendix D: Installing IIS on Windows Server 2008	14

Blade Server Pre-Requisites

To install Blade File Transfer System Server, first check that your server complies with the following pre-requisites:

1. The server is running Windows Server 2003 SP1 or later or Windows Server 2008
2. Internet Information Services (IIS) is installed and ASP.NET is enabled
3. IIS 6 Management Compatibility is installed (Windows Server 2008 only)
4. .NET Framework 2.0 or later is installed (.NET Framework 3.5 SP1 is recommended)
5. Share or folder designated to become the upload directory. You should designate a local directory e.g. C:\Upload or a network share e.g. \\server1\Upload as the upload directory. This is where the users will upload files to and download files from. This directory can reside on a SAN, NAS, or point a file share. You will configure the upload directory within Blade Server Web Administration after the Blade Server installation.

Instructions for installing the pre-requisites are provided in [Informational Appendix C: Installing IIS and ASP.NET on Windows Server 2003](#) and [Informational Appendix D: Installing IIS on Windows Server 2008](#).

Network Pre-Requisites

If you intend to use Blade over the internet, configure your firewall so that the server is accessible from the internet on port 80 or 443 using HTTP or HTTPS protocols.

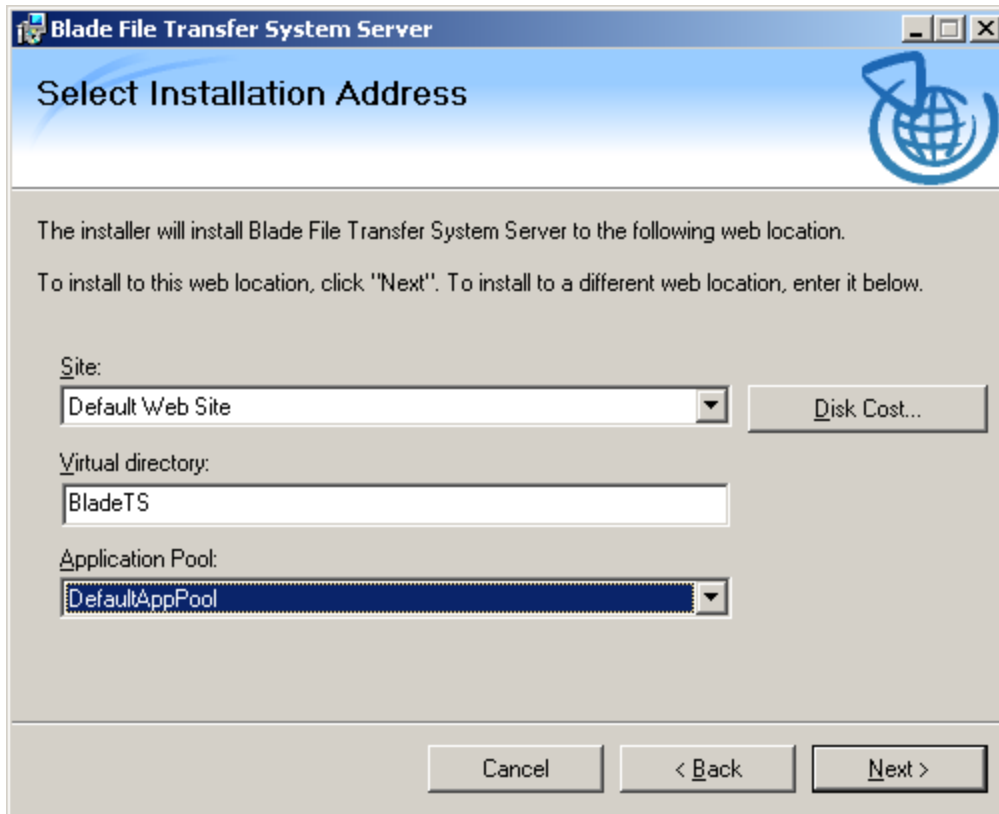
Supported Firewalls:

- Most traditional and NAT-type firewalls are supported
- Microsoft ISA Server Supported
- Port 80 or 443 default
- Custom port numbers supported

Installing the Blade Server

To install the Blade File Transfer System Server, use the following checklist:

1. Navigate to Blade installation media, and navigate to **\Server** folder.
2. Run the appropriate server MSI (32-bit or 64-bit)
3. On the Welcome page click **Next**.
4. If you agree to the license agreement, click **I Agree**, and then click **Next**.
5. Choose the install location (we recommend you keep the defaults, however, you can re-name the virtual directory and choose an alternate web site or port number if you choose to).



Click **Next** twice and then click **Finish**.

Blade Server is now installed and needs to be configured.

Configure IIS – Windows Server 2003

You must follow the procedure below to configure Blade File Transfer System Server on Windows Server 2003.

1. Click **Start | Administrative Tools | Internet Information Services**.
2. In **Internet Information Services Manager** snap-in, expand the IIS Server and then expand **Application Pools**.
3. Right-click Application Pools, click **New** and then click **Application Pool**.
4. In Add New Application Pool box, in **Application Pool ID** box type **BladeTS** and then click **OK**.
5. In Internet Information Services snap-in expand the IIS Server and then expand the website where Blade File Transfer System is installed (Default Web Site by default).
6. Under the website right-click **BladeTS** virtual directory and then click **Properties**.
7. In **Application Pool** dropdown select **BladeTS**.
8. Click the **ASP.NET** tab and in **ASP.NET version** dropdown select **2.0.x**.
9. Click **OK** to save your changes.

Configure IIS – Windows Server 2008

You must follow the procedure below to configure Blade File Transfer System Server on Windows Server 2008.

1. Click **Start | Administrative Tools | Internet Information Services (IIS) Manager**.
2. In IIS Manager, expand the IIS Server and click **Application Pools**.
3. On the right hand side, in the Actions pane click **Add Application Pool**
4. Right-click **Application Pools** | click **New** and then click **Application Pool**.
5. In the Add Application Pool dialog enter the following settings and click OK:
Name: **BladeTS**
.NET Framework version: **.NET Framework v2.0.x**
Managed pipeline mode: **Classic**
Start application pool immediately: **Yes**
6. In IIS Manager, expand the IIS Server | expand **Sites** | expand the **Default Web Site** | click **BladeTS** (or the web site and virtual directory you have installed Blade Server into).
7. On the right hand side, in the Actions pane click **Basic Settings**.
8. In the Edit Application dialog select the **BladeTS** application pool and click OK.

Configure Authentication - Windows Server 2003

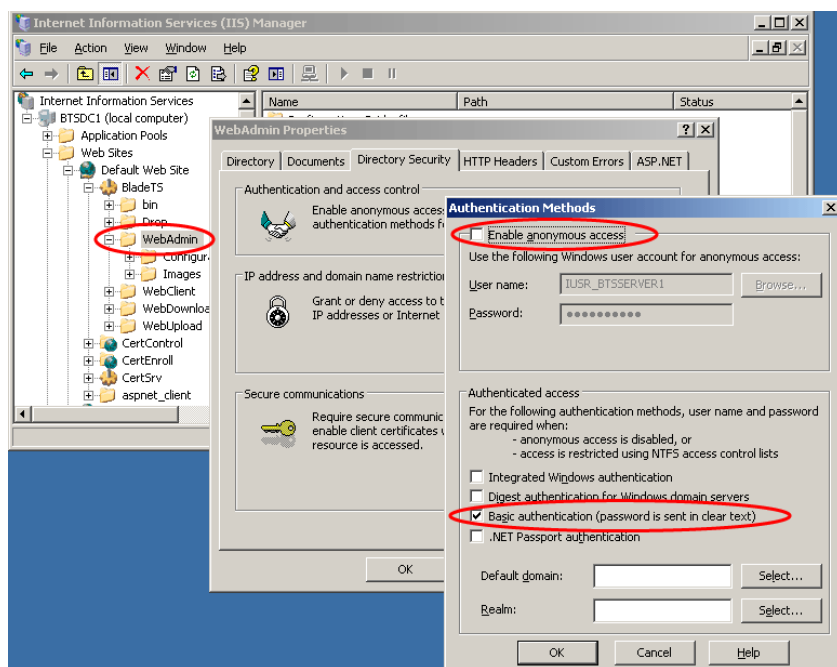
Please configure IIS authentication for each of Blade File Transfer System Server virtual directories as shown in the following table.

Virtual Directory	IIS Security Setting
/BladeTS	Basic
/WebAdmin	Basic
/Drop	Basic
/WebClient	Anonymous
/WebUpload	Anonymous
/WebDownload	Anonymous

How do you set IIS authentication? On Windows Server 2003 use the following instructions:

1. In **Internet Information Services** snap-in expand the IIS Server and then expand the website where Blade File Transfer System is installed (Default Web Site by default).
2. Under the website right-click the virtual directory (e.g, **BladeTS**) virtual directory and then click **Properties**.
3. Click the **Directory Security** tab, under **Anonymous Access and Authentication Control** click **Edit**. Select the required authentication e.g. Anonymous or Basic authentication, and un-select all other types of authentication.
4. Click **OK**.

The following screenshot shows how to set authentication on the the WebAdmin virtual directory.



On Windows Server 2008 use the following instructions:

1. In IIS Manager, expand the IIS Server | expand **Sites** | expand the **Default Web Site** | click **BladeTS** (or the web site and virtual directory you have installed Blade Server into).
2. In the Features view (middle pane), double-click **Authentication**.
3. Right-click **Anonymous Authentication** and then click **Disable** (or **Enable** for WebClient, WebUpload, WebDownload).
4. Right-click **Basic Authentication** and then click **Enable** (or **Disable** for WebClient, WebUpload, WebDownload).
5. In the Actions pane click **Apply**.
6. Repeat for the remainder of the virtual directories.

Detailed information on Blade Server virtual directories and recommended security settings are described in [Informational Appendix B: Virtual Directory Security Settings](#).

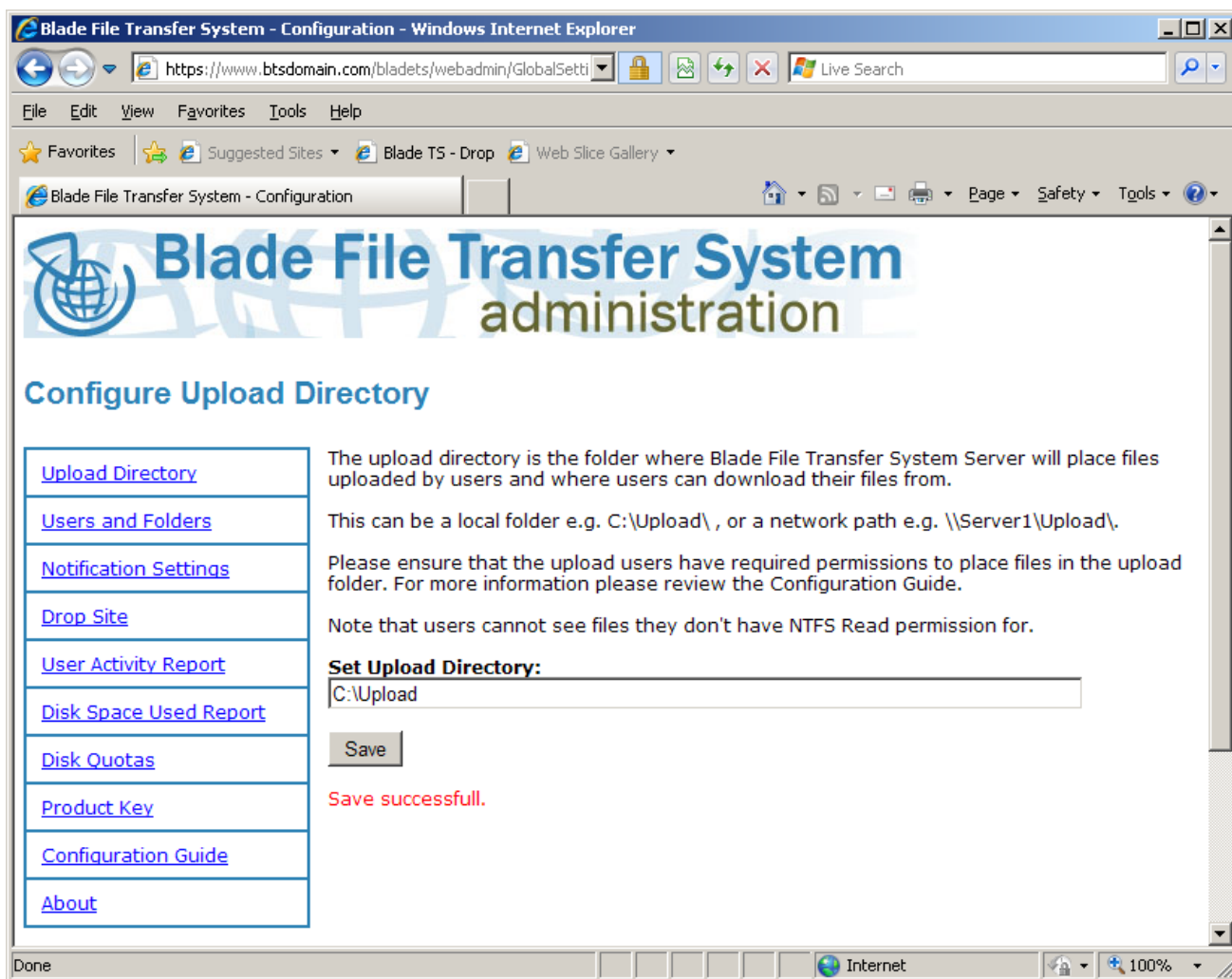
Configure Blade Server Settings

Follow the procedure below to configure Blade File Transfer System settings like upload directory, e-mail notifications, product key etc:

Set the Upload Directory.

This is the directory you have designated earlier, where users will upload files to and download files from.

1. On the Blade server open the Blade Web Administration (click **Start | All Programs | Blade | Blade File Transfer System Server | Web Administration**).
2. You will be prompted for credentials. Log on as a user account that has administrative access to this server.
3. Click the Upload Directory link, set the Upload directory and click **Save**.



Enable / Disable the Drop Site.

1. On the Blade server open the Blade Web Administration (click **Start | All Programs | Blade | Blade File Transfer System Server | Web Administration**).
2. Click the **Drop Site** link, choose to enable or disable and click **Save**. Once saved, click the Drop Site link again to refresh.

Configure Notification Settings. If you wish to receive e-mail notifications when a user uploads files to your server, or if you wish to allow users to notify themselves by e-mail when their transfer is complete, configure e-mail notifications.

IMPORTANT: If you wish to view user activity reports, you must log user activity to an xml log file. You must give all Blade Users write permissions to the directory containing this file. To do this, in Windows Explorer navigate to the directory that will host the file e.g. C:\BladeTSLog. Right-click the folder | click **Properties** | **Security**. Add the Users group and ensure they have **Write** permissions to this folder.

1. On the Blade server open the Blade Web Administration (click **Start** | **All Programs** | **Blade** | **Blade File Transfer System Server** | **Web Administration**).
2. Click the **Notification Settings** link, enter your settings and click **Save**. Once saved, click the E-Mail Notifications link again to refresh.

The screenshot shows a web browser window titled "Blade File Transfer System - Configuration - Windows Internet Explorer". The address bar shows the URL "https://www.btsdomain.com/bladets/webadmin/EMailNotifica". The page content includes a navigation menu on the left with links: Upload Directory, Users and Folders, Notification Settings, Drop Site, User Activity Report, Disk Space Used Report, Disk Quotas, Product Key, Configuration Guide, and About. The main content area is titled "Configure E-Mail Notifications" and contains the following text and form fields:

Choose to notify someone by e-mail when a file is successfully uploaded by Blade Transfer Services. You must enter a valid SMTP server that accepts SMTP connections from this web server for notifications to work.

Notify this person by e-mail

Notification E-Mail Address (send notifications to this address):
administrator@btsdomain.com

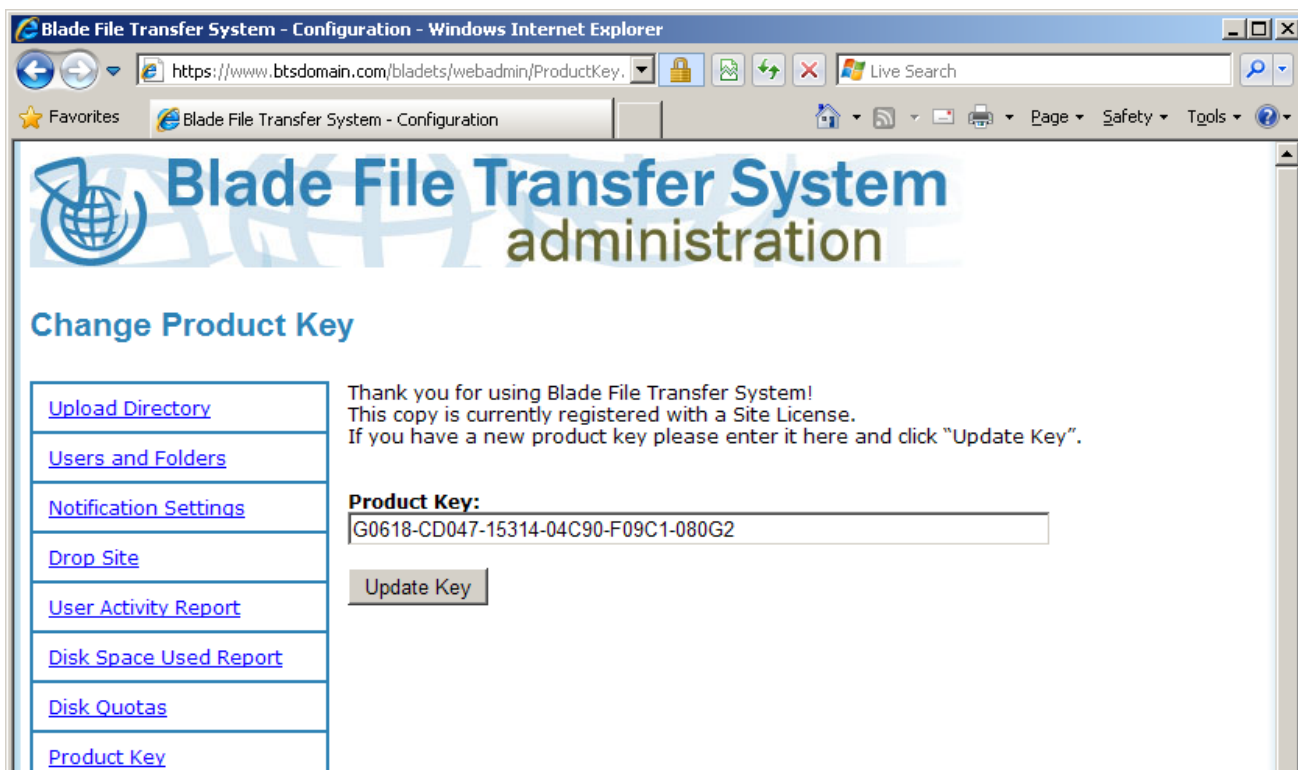
From E-Mail Address (notifications appear to come from this address):
BladeTransfer@btsdomain.com
e.g. blade@mycompany.com

SMTP Server FQDN or IP Address:
mail.btsdomain.com

Log File Location
C:\BladeTSLog\BladeTSLog.xml
e.g. C:\Logs\BladeTSLog.xml. All Blade users must have write permissions to this file.

Configure Product Key. Register your Blade Server with a valid product key.

1. Click the **Product Key** link, enter your product key and click **Update Key**. Once saved, click the Product Key link again to refresh.



Configure Secure Sockets Layer (SSL) – Windows Server 2003

Follow the procedure below to configure Blade File Transfer System to be accessible over SSL on Windows Server 2003. Your Blade URL will start with https:// and SSL encryption will apply to all transfers:

1. Click **Start | Administrative Tools | Internet Information Services**.
2. In Internet Information Services snap-in expand the IIS Server and then expand the website where Blade File Transfer System is installed (Default Web Site by default).
3. Under the website right-click **BladeTS** virtual directory and then click **Properties**.
4. Click the **Directory Security** tab, under **Secure communications** click **Edit** and check **Require Secure Channel**. Click **OK**.

Note: if you complete the previous step, the url for Blade will start with https://, otherwise it will start with http:// i.e. https://www.mycompany.com/BladeTS vs http://www.mycompany.com/BladeTS

Note: If **Secure communications** option is not available, you have not installed an SSL certificate on this web server. To learn about SSL certificates, visit **Obtaining Server Certificates (IIS 6.0)** at

Configure Secure Sockets Layer (SSL) – Windows Server 2008

Follow the procedure below to configure Blade File Transfer System to be accessible over SSL on Windows Server 2003. Your Blade URL will start with https:// and SSL encryption will apply to all transfers:

1. Click **Start | Administrative Tools | Internet Information Services (IIS) Manager**.
2. In IIS Manager, expand the IIS Server | expand **Sites** | click **Default Web Site**.
3. On the right hand side, in the Actions pane click **Edit Site Bindings**.
4. In the Site Bindings box click Add.
5. In Add Site Binding enter the following settings and click OK:
Type: **https**
SSL Certificate: **your SSL Certificate**
Port: **443**
6. In IIS Manager, expand the IIS Server | expand **Sites** | expand **Default Web Site** | click **BladeTS** (or the web site and virtual directory you have installed Blade Server into).
7. In the Features view (middle pane), double-click **SSL Settings**.
8. Check the **Require SSL** checkbox (for greater security you can also check **Require 128-bit SSL**, though it may not be supported by older client computers).
9. In the Actions pane click **Apply**.

Note: if you complete the previous step, the url for Blade will start with https://, otherwise it will start with http:// i.e. <https://www.mycompany.com/BladeTS> vs <http://www.mycompany.com/BladeTS>

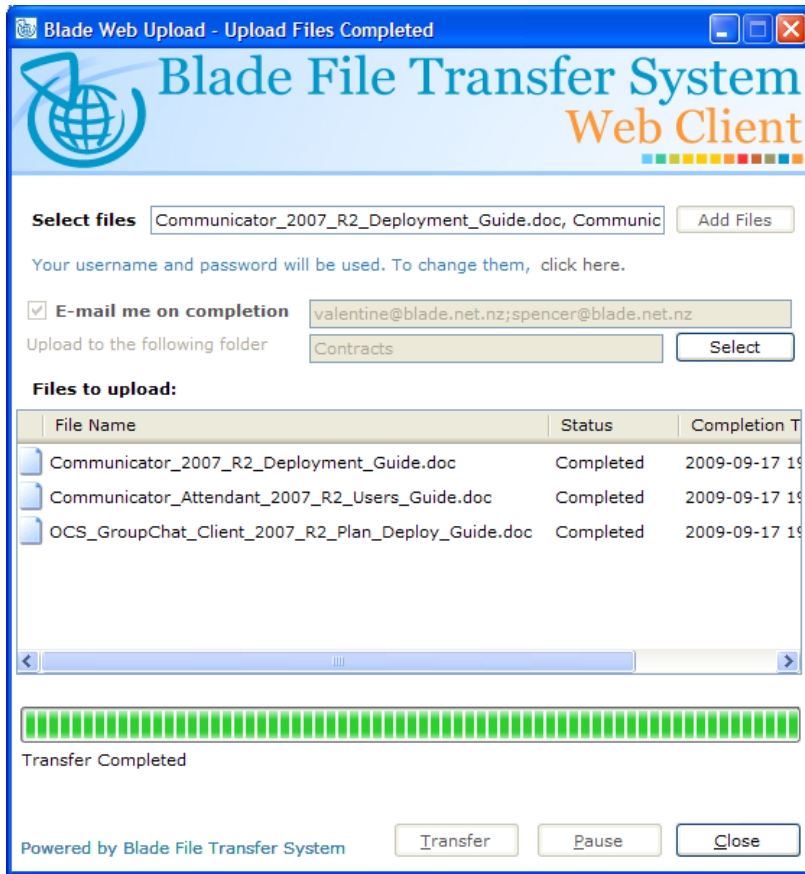
Note: If **SSL Certificate** option is not available, you have not installed an SSL certificate on this web server. To learn about SSL certificates, visit **Configuring Server Certificates in IIS 7** at [http://technet.microsoft.com/en-us/library/cc732230\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc732230(WS.10).aspx)

Test File Upload and Download using WebClient

Follow the procedure below to test file upload and download using WebClient:

Test the Blade Web Upload client

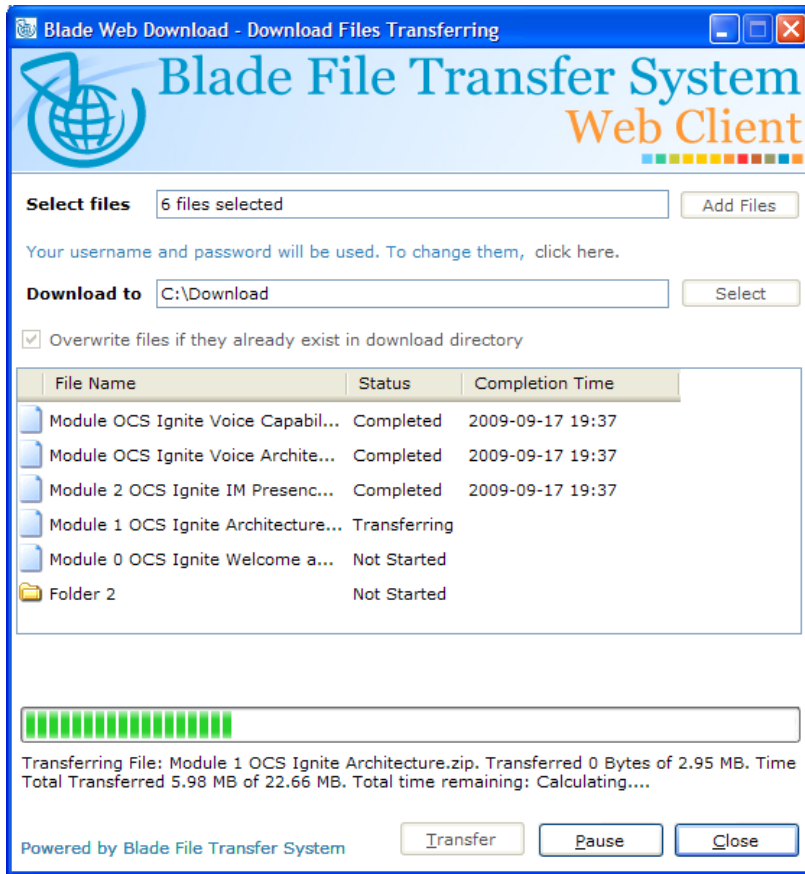
1. On the Blade server open the Blade Web Client (click **Start | All Programs | Blade | Blade File Transfer System Server | Transfer Files**) or open a web browser and navigate to [http\(s\)://<server url>/BladeTS/WebClient](http(s)://<server url>/BladeTS/WebClient).
2. Click **Upload Files**.
3. Wait for the application to deploy, then attempt to upload files to your server.



4. Ensure that the files upload successfully.

Test the Blade Web Download client

1. Open a web browser and navigate to [http\(s\)://<server url>/BladeTS/WebClient](http(s)://<server url>/BladeTS/WebClient).
2. Click **Download Files**.
3. Wait for the application to deploy, then attempt to download files from your server.



4. Ensure that the files download successfully.

Known Issue – Symantec Anti Virus software

When users upload files to the Blade Server, the temporary files go into the Upload\Temp directory (i.e. the Temp folder within the Upload Directory). Some users experience problems with Symantec Anti Virus software locking the temporary files while they are still being written to. This causes users uploads to fail.

To overcome this issue, exclude the Upload\Temp directory from Symantec virus scanning. Once the files are uploaded, they are automatically moved to the Upload directory where they can be virus scanned etc.

Informational Appendix A: File Security and Permissions

Blade allows users to upload files to the server and download files from the server. Files are placed into the upload directory, and are downloaded from the upload directory, via means of a web service. Please use the following guidance when applying file permissions:

Running the Blade Server with Basic Authentication

In this case, users must enter username and password to upload and download files. These credentials are authenticated in either Active Directory, or the local IIS server (it is up to you). These user accounts must have Write NTFS permissions to the Upload directory (or their own subfolder) and the Upload\Temp directory.

Note: if a user does not have Read permission to a file or folder, they will not be able to see or download that file.

Running the Blade Server with Anonymous Authentication

In this case, users do not enter a username and password to upload and download files from your server— anyone can do so. The account accessing the files is Network Service. It must be given Write NTFS permissions to the Upload directory (or their own subfolder) and the Upload\Temp directory.

Note: if Network Service does not have Read permission to a file or folder, users will not be able to see or download that file / folder.

Note: you can change the Network Service to another account, on the properties of the BladeTS web application pool, Identity tab.

Support and Troubleshooting

Your Blade File Transfer System server comes with 12 months next-business day e-mail support facility. You can contact support at www.blade.net.nz/Support.aspx or e-mail support@blade.net.nz. To assist us in the troubleshooting process, obtain the file Error.log (could also be named Error[Date and Time].log). This file is located in the Upload directory. The file may not always be present, depending on the issue. Thank you and we would love to hear from you!

Informational Appendix B: Virtual Directory Security Settings.

Blade File Transfer System Server consists of several IIS virtual directories. You must set authentication on these directories, so that users are required to authenticate when uploading and downloading files. These settings are listed below.

- **/BladeTS virtual directory.** Users connect to the Blade web service in this virtual directory to upload and download files. If you want users to authenticate (enter their username and password) when uploading and downloading files, set the authentication to Basic. If you want

anyone to upload and download files to your server using Blade File Transfer System client software, set the authentication to Anonymous. **Recommended security: Basic.**

- **/WebAdmin virtual directory.** Administrators connect to the WebAdmin virtual directory to configure settings for this Blade Server. We recommend that you set the authentication to Basic for this virtual directory. **Recommended security: Basic.**
- **/Drop virtual directory.** Users connect to the Drop virtual directory to download files from this Blade Server, without installing any Blade software. By default, the Drop virtual directory is disabled. If you enable this feature, you should set the authentication on it as per your requirements. If you want users to authenticate (enter their username and password) when downloading files, set the authentication to Basic. If you want anyone to download files to your server using the Drop site, set the authentication to Anonymous. **Recommended security: Basic.**
- **/WebClient virtual directory.** The WebClient virtual directory contains an HTML page pointing users to WebUpload and WebDownload ClickOnce applications. Users can use these links to upload and download files to the Blade Server without installing the full-featured client. If you want users to authenticate to use these links set the authentication to Basic. If you want anyone to be able to access the WebDownload and WebUpload client software, set the authentication to Anonymous. Note that users will be required to authenticate when uploading / downloading files if you have configured the BladeTS virtual directory for Basic authentication. The authentication on the /WebClient virtual directory controls access to the link page only. **Recommended security: Anonymous.**
- **/WebUpload virtual directory.** This virtual directory contains the ClickOnce deployment for the WebUpload client software. The authentication for this virtual directory must be set to anonymous for Blade File Transfer System to work. Note that users will still be required to authenticate when uploading files if you have configured the BladeTS virtual directory for Basic authentication. **Recommended security: Anonymous.**
- **/WebDownload virtual directory.** This virtual directory contains the ClickOnce deployment for the WebDownload client software. The authentication for this virtual directory must be set to anonymous for Blade File Transfer System to work. Note that users will still be required to authenticate when uploading files if you have configured the BladeTS virtual directory for Basic authentication. **Recommended security: Anonymous.**

Informational Appendix C: Installing IIS and ASP.NET on Windows Server 2003

To install Internet Information Services (IIS) on Windows Server 2003, use the following procedure:

1. Log on to the server as an account with local administrator rights
2. Click **Start | Control Panel | Add or Remove Programs | Add / Remove Windows Components**
3. Select **Application Server** and click **Details**.

4. Select **Internet Information Services (IIS)** and click **Details**.
5. Check the **World Wide Web Service** box and click **OK** twice. Click **Next** to install **IIS**.
6. To install ASP.NET simply install the .NET Framework (if it isn't installed already). Blade Server requires that .NET Framework 2.0 or later is installed (.NET Framework 3.5 SP1 or later is recommended).
7. To enable ASP.NET click **Start | Administrative Tools | Internet Information Services**.
8. In Internet Information Services snap-in, expand the IIS Server and then click **Web Service Extensions**.
9. If ASP.NET v2.* is listed as Prohibited, in the right pane click **ASP.NET v2.*** and then click **Allow**.

To download and install the Microsoft .NET Framework visit <http://www.microsoft.com/NET/>

Informational Appendix D: Installing IIS on Windows Server 2008

To install Internet Information Services (IIS) on Windows Server 2008, use the following procedure:

1. Log on to the server as an account with local administrator rights
2. Click **Start | All Programs | Server Manager**.
3. Right-click the **Roles** container and click **Add Roles**.
4. In the **Select Server Roles** screen check the **IIS** checkbox and then click **Next** twice.
5. In Select Role Services dialog check the **ASP.NET** checkbox and choose to add role services required for ASP.NET.
6. In Select Role Services dialog check the **IIS Management Console** and **IIS 6 Management Compatibility** checkboxes and then click **Next | Install**.