# Table of Contents

**Introduction to Secure Ad Hoc Transfer** ............................................................................................. 5

**What's New in Secure Ad Hoc Transfer** .......................................................................................... 6

**Installing Secure Ad Hoc Transfer** ................................................................................................. 7

- Secure Ad Hoc Transfer Module System Requirements .................................................................. 7
- Secure Ad Hoc Transfer Deployment Methods ............................................................................. 7
- Secure Ad Hoc Transfer in the DMZ .............................................................................................. 8
- Secure Ad Hoc Transfer Installation Prerequisites ...................................................................... 9
- BEFORE Installing the SAT Module with IIS 7.0 ........................................................................... 9
- Installing Secure Ad Hoc Transfer ............................................................................................... 11
  - Verify the Microsoft IIS Settings .............................................................................................. 17
- Manually Configuring Microsoft IIS ............................................................................................. 18
- Using SAT on 64-Bit Operating Systems .................................................................................... 21
- Activating Secure Ad Hoc Transfer .............................................................................................. 23
- Upgrading Secure Ad Hoc Transfer ............................................................................................. 24

**Configuring Secure Ad Hoc Transfer** ........................................................................................... 25

- Customizing the Secure Ad Hoc Transfer Web Interface ............................................................. 27
  - Background Color ....................................................................................................................... 27
  - Header Image Dimensions ......................................................................................................... 28
  - Banner Background Style ........................................................................................................... 28
  - Banner Image .............................................................................................................................. 28
- Customizing the Notification E-Mail ............................................................................................... 29
- Configuring Temporary User Account Expiration ...................................................................... 30
- Editing the Configuration File (web.config) ................................................................................ 30
  - IIS Authentication ..................................................................................................................... 40
- Creating a Base64-Encoded Password ........................................................................................... 40
- Specifying Virtual Folders for Ad Hoc Users ............................................................................. 41
- Adding Blacklist and Whitelist Domains ...................................................................................... 42
- Single-Click Authentication .......................................................................................................... 43
- Using SAT with Active Directory ............................................................................................... 43
- Receiving Notifications when Recipients Upload Files ............................................................... 44
- Creating a Timer Rule to Remove Temporary Expired Accounts ............................................... 48
Scheduler (Timer) Event ........................................................................................................... 49
Default Template Locations ..................................................................................................... 52
Specifying HTML or Plain Text E-Mail Format ....................................................................... 52
Creating a Command ............................................................................................................... 53
Enforcing Complex Passwords for Temporary Users ............................................................ 54
Using the HS Module with the Secure Ad Hoc Transfer Module ........................................ 54

Using the Secure Ad Hoc Transfer Module ........................................................................... 57
Sending Files ............................................................................................................................ 57
Smart E-Mail Functionality ....................................................................................................... 58
Including Cc and Bcc Recipients ............................................................................................ 59
Personal Address Book ............................................................................................................. 59
Picking Up Files ....................................................................................................................... 60
Allowing Recipients to Upload Files ....................................................................................... 61
Viewing Reports of SAT Activity ............................................................................................. 61

Troubleshooting Errors in the Secure Ad Hoc Transfer Module ........................................ 62
Failed to Connect to EFT Server ............................................................................................. 62
Ad Hoc Properties Missing ASP.NET Tab ................................................................................. 62
"Current Identity does not have Write Access" ...................................................................... 64
Failed to Access IIS Metabase ................................................................................................. 64
Problem Sending Large Files .................................................................................................. 65
SAT Module Application Error Codes ....................................................................................... 65
INTRODUCTION TO SECURE AD HOC TRANSFER

EFT Server’s Secure Ad Hoc Transfer (SAT) module allows your internal users to send and receive large e-mail file attachments to recipients outside of your organization quickly, reliably, and securely, all without having to manually create or maintain FTP accounts on EFT Server.

The SAT Module works in conjunction with EFT Server to allow users inside an enterprise to transfer files to and from recipients outside the organization with secure authentication, non-repudiation, and auditing capabilities. ASP.NET technology overcomes file-size limits when uploading very large attachments. The Web supports file attachments up to 2GB, which is a limit of HTTP. (If you expect to upload large files, e.g., 1 GB or larger, we strongly recommend that you install EFT Server on the same computer as IIS and edit the value for UploadProtocol in the Secure Ad Hoc Transfer’s Configuration File.)

The process is bidirectional; recipients can securely return files to the sender if the sender grants them permission. Auditing and receipt notifications provide verifiable transfer of data.

An automated process sets up new user accounts, assigns home folders, notifies the recipient that a file is ready to be picked up, audits all transactions, expires old temporary accounts, and finally, deletes expired accounts.

Below is a brief overview of what takes place behind the scenes when users send a file.

1. A user sends an e-mail with an attachment using EFT Server’s Ad Hoc Transfer.
2. Ad Hoc Transfer creates a new temporary account on EFT Server. This temporary account is assigned a random username and password, and expires in seven days.
3. A temporary folder is created and associated with the temporary account. An e-mail is sent to the recipient with a secure hyperlink (HTTPS), a temporary account user name and password, and a list of files available for download.
4. The recipient of the e-mail follows the HTTPS link, enters the temporary user name and password, and connects to the default HTTPS Web interface or the Web Transfer Client. (The link is configured when you install SAT; you can change this link in the SAT configuration file. Refer to Editing the Configuration File (web.config) for details. The variable is URLPattern.)
5. The recipient can now download the files.
6. The recipient can also upload files if this option is enabled by the sender. When files are uploaded, the sender is notified that the uploaded files can be picked up. The recipient uses the same login credentials. After seven days, the temporary account user name and password is disabled, and the disabled temporary account is removed from EFT Server’s file system.
7. If EFT Server has Auditing and Reporting, all of the transactions associated with the Ad Hoc account are logged to EFT Server’s auditing and reporting database for non-repudiation and auditing purposes.
WHAT'S NEW IN SECURE AD HOC TRANSFER

For "What's New" in any version of Secure Ad Hoc Transfer (SAT), refer to the release notes, notes.txt, in the SAT installation folder (by default, C:\inetpub\EFTAdHoc) or the GlobalSCAPE support page http://www.globalscape.com/eft/sat_history.aspx.

The following features were added to version 2 of the SAT module (for use with version 6.x of EFT Server):

- Authentication via Active Directory to pre-populate the From address field and lock it so users cannot change it. This option is configurable in the SAT configuration file. (It is NOT the default behavior.)
- Full transaction logging to ARM. SAT has an option to log each SAT submission/transaction to the ARM database.
- New reports provided for SAT submissions/transactions. (Refer to in the EFT Server User Guide for details.

The following features were added to version 2.1 of the SAT module (for use with version 6.1 of EFT Server):

- Prevents "spoofing" by forcing the From address to the address in Active Directory before sending the message (when authenticating using AD Authentication for the sender).
- Logs the IP address of the sender to the auditing database and will appear in the ARM SAT reports.
- Verifies whether prerequisite applications are installed (IIS version and .NET version) and configuration/IIS role settings are correct before continuing.
- Detects whether IIS 7 is installed and, if it is, extends the maxAllowedContentLength value in IIS's ApplicationHost.config file to 2 GB.
- Added a label to the SendMail form to remind users that they can only send files up to 2 GB (unless SAT is installed on the same computer as EFT Server).
- Supports semicolon delimiter for multiple e-mail send addresses.
INSTALLING SECURE AD HOC TRANSFER

The topics below provide information regarding installing the Secure Ad Hoc Transfer module.

SECURE AD HOC TRANSFER MODULE SYSTEM REQUIREMENTS

The Secure Ad Hoc Transfer (SAT) Module has been tested on Windows XP Professional, Windows Server 2003, and Windows Server 2003 x64, and requires the following:

- A server computer running GlobalSCAPE EFT Server, version 6 or newer
- Microsoft Internet Information Services (IIS) Web Server version 5, 6, or 7 (SAT must be installed on same computer as .NET) To use SAT with IIS7, you must configure several options BEFORE you install the software.
- Microsoft .NET Framework Runtime, version 3.5 or newer (SAT must be installed on same computer as .NET) If you are using IIS7, configure IIS options BEFORE you install .NET.

Microsoft .NET 3.5 is supported on the following operating systems:
- Microsoft Windows XP
- Microsoft Windows Server 2003
- Windows Vista
- Windows Server 2008

- An SMTP mail server
- If SAT is installed on a separate computer from EFT Server, EFT Server must be configured for remote administration.

To enable SAT to work on 64-bit operating systems, refer to Using SAT 2.0 on 64-Bit Operating Systems.

SECURE AD HOC TRANSFER DEPLOYMENT METHODS

The Secure Ad Hoc Transfer (SAT) Module is installed on the IIS server computer. The IIS server computer can be on the same server computer where EFT Server is running, or on a separate computer. To minimize system resources, it is recommended that EFT Server and IIS be installed on the same server computer; however, if system resources are not a factor, then placing EFT Server and IIS on separate server computers may facilitate installation and setup.

Common Deployment Methods

1. **Place IIS with SAT inside your network.** Access to the SAT Web interface is limited to internal users who can exchange files with external users. This method can be used with or without DMZ Gateway Server.

2. **Place IIS with SAT in the DMZ.** Access to the SAT Web interface is available to external users who can exchange files with internal users or other external users. GlobalSCAPE recommends against placing the IIS server with SAT in the DMZ to prevent possible misuse of the SAT module.
Secure Ad Hoc Transfer Module for EFT Server v6.1

If you plan to install EFT Server and IIS on the same system, you must have:

- HTTPS enabled on EFT Server at the Site level.
- Your EFT Administrator username and password
- EFT Server and IIS both running before the Secure Ad Hoc Transfer module is installed.

If you plan to install EFT Server and IIS on different systems, you must have:

- HTTPS enabled on EFT Server at the Site level
- Your EFT Administrator username and password
- The remote administrator enabled in EFT Server.
- EFT Server’s IP address accessible from EFT Server running IIS
- EFT Server and IIS both running before the Secure Ad Hoc Transfer module is installed

HTTPS is required on EFT Server to enable recipients to pick up their files.

One common deployment scheme is to place both IIS and EFT Server inside your network. Only internal users are able to access the Secure Ad Hoc Transfer Web interface and exchange files with users outside the network.

The architectural diagram below demonstrates this setup with EFT Server and IIS both on separate boxes. It also assumes the use of the DMZ Gateway; without it, you would need to configure the solution differently, so that recipients can reach EFT Server.

1. The sender, inside your network, connects to the Web form provided by IIS running the Secure Ad Hoc Transfer module page.
2. Secure Ad Hoc Transfer on IIS then offloads the file to EFT Server, creates a notification message, and sends that directly to the recipient through your SMTP server.
3. The recipient connects using the link-back https hyperlink to EFT Server to download the available files and, if applicable, uploads files back to EFT Server for later pick-up by the originator (sender).

SECURE AD HOC TRANSFER IN THE DMZ

You can deploy Secure Ad Hoc Transfer in the DMZ so that clients or partners can initiate a send either to one of your users, or to a third party. GlobalSCAPE recommends against this approach to avoid potential misuse of the Secure Ad Hoc Transfer module.
Troubleshooting Errors in the Secure Ad Hoc Transfer Module

Before installing the application, review the System Requirements and decide on a Deployment Method, then review the Installation Prerequisites, below.

SECURE AD HOC TRANSFER INSTALLATION PREREQUISITES

Before installing the SAT module, the following tasks must be completed:

- Both EFT Server and IIS must be installed, configured, and running before installing the SAT module. The v6.1 installer detects which version of IIS is installed.

  If you expect to upload large files, e.g., 1 GB or larger, we strongly recommend that you install EFT Server on the same computer as IIS, and edit the web.config file as necessary per the instructions in Secure Ad Hoc Transfer’s Configuration File.

- If EFT Server and IIS are not running on the same computer, you must ensure that IIS can reach EFT Server via the EFT Server administration port. By default, the administration port is set to 1100.

- IIS and .NET Framework 3.5 must be installed, configured, and running before installing the SAT module.
  (If you have already installed .NET, but not IIS, be sure to register IIS with .NET after you install IIS.)

- Before installing the SAT module, you should have the following information available:
  - The EFT Server administrator account user name and password.
  - The EFT Server IP address and administration port number. (By default, the administration port is set to 1100.)
  - The SMTP server IP address and port number.
  - A default From e-mail address that can be used if the sender fails to enter an address.
  - The SMTP server authentication credentials, if required.
  - A SAT Module activation serial number. (Either trial or full version)

- The following settings should be configured in EFT Server before installing the SAT module:
  - Remote Administration should be turned on in EFT Server.
  - HTTPS protocol must be enabled at the EFT Server Site level.

To test the connection

1. On the IIS server, open a command prompt.

2. Type telnet <IP_address> <port_number> then press ENTER. For example type:

   telnet 192.168.20.123 1100

   If EFT Server is not reachable, the Telnet response is Connect failed.

BEFORE INSTALLING THE SAT MODULE WITH IIS 7.0

In order to install SAT 2.0 correctly with IIS 7.0 you will need to enable (select) several IIS features.

On operating systems other than Windows 2008, you will need to install .NET Framework 3.5 AFTER these features are enabled.
To enable features necessary for the SAT module to run properly

1. Open the **Programs and Features** control panel and click the **Turn Windows features on or off** link on the left.

2. In the **Windows Features** dialog box, expand the **Internet Information Services** node.

3. Expand the **Web Management Tools** node, and the **IIS 6 Management Compatibility** node and select the following check boxes:
   - IIS Metabase and IIS6 configuration compatibility
   - IIS Management Console

4. Expand the **World Wide Web Services** node and the **Application Development Features** node, and select the following check boxes:
   - .NET Extensibility
   - ASP.NET
   - ISAPI Extensions
   - ISAPI Filters

5. Expand the **Common Http Features** node and select the following check boxes:
   - Default Document
   - HTTP Errors
   - Static Content

6. Expand the **Security** node and select the following check boxes:
   - Request Filtering
   - Windows Authentication

The illustration on the next page shows the necessary features enabled:
INSTALLING SECURE AD HOC TRANSFER

Before installing the application, review the System Requirements, decide on a Deployment Method, review the Installation Prerequisites, then read the entire procedure below.

- The Secure Ad Hoc Transfer (SAT) installation program automatically detects the presence of IIS, .NET Framework, previous versions of the SAT module, and EFT Server, and prompts for required information to configure the services. Install EFT Server before installing the SAT module, and make note of the EFT Server name, IP address, username, and password, because you will need to provide this information in the SAT installer.
Secure Ad Hoc Transfer Module for EFT Server v6.1

- If a previous version of the SAT module is installed on the computer, you must uninstall it before installing the newer version. Before installing the new version, verify that the Ad Hoc virtual directory in IIS (EFTAdHoc by default) and the Ad Hoc installation directory (C:\InetPub\EFTAdHoc) were removed. Installing EFT Server, Microsoft IIS, and .NET Framework on the same physical computer expedites the installation process, but it is not required.

- If you are not installing SAT on the same computer as EFT Server:
  - Provide IIS a direct route and IP address to EFT Server.
  - Enable in EFT Server so that the installer can remotely configure EFT Server to use SAT.
  - must be enabled at the Site level so that the SAT scripts running on IIS can communicate with EFT Server.

Before installing the SAT module, perform the steps below in the order listed. If you do not follow each of the steps below in the order listed, the SAT module might not function as you intend:

  - Review the System Requirements and decide on a Deployment Method.
  - Review the Installation Prerequisites.
  - On operating systems other than Windows 2008, ensure IIS is installed BEFORE ASP.NET is installed. If ASP.NET is installed before IIS is installed, you must provide the network service with write access to the framework directory (e.g., C:\WINDOWS\Microsoft.NET\Framework\v3.5). Ensure that ASP.NET is installed and registered. See AdHoc Properties Missing ASP.NET Tab for details of registering ASP.NET.
  - If you are installing SAT with IIS7, configure IIS using the instructions in BEFORE Installing the SAT Module with IIS7.

To install Secure Ad Hoc Transfer

1. Copy the installer to the IIS computer.
2. Double-click the installer. The Welcome page appears.
   
   ![Welcome to the Secure Ad Hoc Transfer Module Setup Wizard](image)

3. Click Next. The License Agreement appears.
4. Read the license agreement and accept it by clicking Yes. (If you do not accept the license agreement, the installer exits.) The **Choose Install Location** page appears.

5. Specify the folder in which to install the SAT module (e.g., `C:\inetpub\wwwroot\EFTAdHoc`), then click **Next**. The **Install Trial or Full** page appears.
6. Do one of the following, then click **Next**:

   - **If you are evaluating the SAT Module prior to purchase, click Trial Version, then skip to step 8.**
   
   > The trial version of SAT is not time limited; however, it is limited to ten e-mails with one attachment each, per IIS session.

   - **If you have purchased the SAT Module, click Full Version. The Activation page appears.**

     If a message appears stating that the installer did not detect the correct version of the Microsoft .NET Framework, click Yes to exit the installer and open the Web browser to the .NET Framework Developer Center. If you know that .NET is installed, you can click No to continue with the installation, then resolve the error later. Refer to AdHoc Properties Missing ASP.NET Tab for details, if necessary.

7. **If you selected Full Version, type or paste the SAT Module activation serial number, then click Next. The Configure IIS page appears.**
8. Specify a **Web Site** and the **Virtual Folder** name (the default is **EFTAdHoc**) to use for the SAT components, then click **Next**. The **EFT configuration parameters** page appears.

![Secure Ad Hoc Transfer Module Setup](image)

9. Provide the **EFT Server name/IP address**, **Server Port**, and **EFT Server Administrator User Name** and **Password**, then click **Next**. The **EFT Site Configuration Parameters** page appears.

![Secure Ad Hoc Transfer Module Setup](image)

10. Specify the **EFT Server Site Name** and a new, unique **User Settings Template** name (the default is **EFTAdHoc**) that will be used only for SAT, and the **External Domain Name** for EFT Server. This is the external server address used to access EFT Server. **IMPORTANT**: If you are also using DMZ Gateway, then use that address instead. Because e-mail recipients can be on an external network, you should use a DNS instead of the actual IP address. For example, type **myfileserver.com** (which might map to https://10.0.0.100:444).
11. Click **Next** to continue. The **SMTP Mail Server Parameters** page appears.

12. Type the SMTP **Server Name/IP** address, **Server Port**, and **Default Sender Address** (e-mail). If mail server authentication is required, click **Server Requires Authentication**, then type the **Administrator User Name** and **Administrator Password** used to connect to the mail server, then click **Next**.

13. If you want to test the SMTP mail server configuration settings, you can click **Test** to send an e-mail to an accessible account. Provide the e-mail address for the test e-mail, then click **Install**.

14. Click **Yes** if the e-mail was successful. Click **No** if the e-mail was not received, then verify your SMTP settings.

15. Installation of the SAT module is complete. A few additional steps are necessary:
   a. Enable **automatic notification of uploads** and **user clean-up** events in EFT Server.
   b. Verify that the Microsoft IIS settings are configured correctly, as described below.
The help file, adhoc.chm, is available from the Start menu and in C:\inetpub\EFTAdHoc\Help.

VERIFY THE MICROSOFT IIS SETTINGS

If EFT Server and IIS are NOT running on the same computer, copy to the EFT Server computer the EFTAdHoc folder (by default, C:\inetpub\wwwroot\EFTAdHoc\) and all files and subfolders.

Note the web.config file at the bottom of the file list. If this file does not exist, the SAT module will not be able to connect to EFT Server. The web.config file provides the configuration for the EFTAdHoc properties in IIS.
To verify IIS settings

1. Open the IIS Manager, right-click the **EFTAdHoc** virtual folder, then click **Properties**.

2. On the **ASP.NET** tab, make sure **ASP.NET version 2.0.50727** (or newer) is selected. (If the **ASP.NET** tab is not displayed, refer to **AdHoc Properties Missing ASP.NET Tab**.)

3. Click **Edit Configuration**. Refer to **Editing the Configuration File** for details.

**MANUALLY CONFIGURING MICROSOFT IIS**

The steps below are performed automatically when you install the SAT module. The procedure is provided here in case changes are made to the IIS configuration that cause Secure Ad Hoc Transfer to stop working and you need to restore the defaults.

If you are using SAT on a 64-bit operating system, refer to **Using SAT 2.0 on 64-Bit Operating Systems**.

**IUSR_<computer name>** account needs write/modify permission to `/temp/` folder if logs and upload path is set to default configuration in the `web.config`.

If authentication is enabled for the Site, the **Authenticated Users** group needs permission instead of the **IUSR** account.
1. The physical folder where Secure Ad Hoc Transfer is installed must have appropriate permissions set so that the anonymous user account for IIS (IUSR_<computer name>) has **Read & Execute**, **List Folder Contents**, and **Read** access to the entire folder tree.

2. The installer creates a new IIS Virtual Directory for Secure Ad Hoc Transfer under the website you selected when SAT was installed. If you want the collection of ASP pages to be accessible to only a subset of users (for example, only those users on your internal network), set up 2 IP addresses on the EFT Server computer (if running EFT Server and IIS on the same box). For example, you might have a public IP address that is Internet accessible through the router/firewall/NAT, while also having an internal IP address that is only routable by those computers on your network.

   If you do not have two NIC cards in your computer, you can still create multiple IP addresses using the **TCP/IP configuration of the computer. Refer to the Windows Operating System documentation on how to set up multiple IP addresses on a single network interface card.**
3. The Home Directory of the new IIS Web Site must point to the location where the SAT module was installed.

4. The Secure Ad Hoc Transfer installer adds sendmail.aspx to the list of filenames to the Documents tab for the virtual directory when it is installed. This allows IIS to execute sendmail.aspx automatically when a user navigates to this Site's URL without explicitly specifying a document.

5. On the ASP.NET tab, you can view/set the Secure Ad Hoc transfer module configuration. See Secure Ad Hoc Transfer's Configuration File for details.
USING SAT ON 64-BIT OPERATING SYSTEMS

The Secure Ad Hoc Transfer SAT module can be installed on Windows Server 64-bit OS. However, you must first enable 32-bit applications to run on the system. Procedures are provided below for IIS 6 and IIS 7.

Ideally, you will install IIS first, then .NET, then SAT. If you have already installed IIS, .NET, and SAT, you do not need to uninstall and reinstall everything. You will just need to allow 32-bit applications and run the ASP.NET registration tool (in that order), as described below. For other IIS7 and SAT errors, refer to Knowledge Base article Q10510 - FIX: Secure Ad Hoc Transfer errors with Microsoft IIS 7.

Using SAT with IIS 6 on a 64-bit OS

1. Set IIS to allow enabling 32-bit applications. At a command line, type the following:
   
   C:\Inetpub\AdminScripts\cscript.exe adsutil.vbs set W3SVC/AppPools/Enable32BitAppOnWin64 true

2. Allow 32-bit in the IIS Manager:
   a. In the IIS Manager tree, click Web Services Extensions.
   b. In the right pane, right-click ASP.NET v2.0.50727 (32-bit), then click Allowed.
   c. Close the IIS Manager.

3. Reregister IIS. At a command line, type the following:
   
   C:\windows\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis.exe -i

Using SAT with IIS 7 on a 64-bit OS

1. In the IIS Manager, click Application Pools.

2. Right-click the application that is hosting SAT, then click Advance Settings.
3. The **Advanced Settings** dialog box appears. Click the **Enable 32-Bit Applications** setting and change it to **True**.

4. Restart the worker process (w3wp.exe).
When you first install the Secure Ad Hoc Transfer module, you are given the choice of installing a Full or Trial version. The trial version is not time limited, but file sender operations are limited to ten per IIS session and a single file at a time. When you are ready to activate the SAT module, you have to re-execute the installer and click Modify to install the Full version of the product.

To activate the full version

1. Execute the installer and accept the license agreement.

2. Click Modify, then click Next.

3. Click Full Version, then click Next.
4. Provide your Secure Ad Hoc Transfer module serial number (on your invoice), then click Next. The full version of Secure Ad Hoc Transfer installs.

**UPGRADING SECURE AD HOC TRANSFER**

Whether you are upgrading to a newer version of the Secure Ad Hoc Transfer (SAT) module or upgrading EFT Server, consider the following information:

- It is very important that SAT have the same version of SFTPCOMInterface.dll that the EFT Server to which SAT is connecting is using. Upgrading EFT Server might require also updating the SFTPCOMInterface.dll for the SAT module.

- If EFT Server and SAT are on the same computer, then the upgrade process for EFT Server will register the new .dll on the computer and will be used by SAT; however, in this case the IIS service must be restarted. This is important so that ASP.NET (hosted by the "aspnet_wp.exe" process) will release any references to the existing COM object and reload the new one.

*By default, SFTPCOMInterface.dll is stored in the EFT Server installation directory and in C:\Inetpub\EFTAdHoc for the SAT module.*
To upgrade Secure Ad Hoc Transfer

1. Run the installer for the new version. Refer to Installing Secure Ad Hoc Transfer for details, if necessary.

   ![Secure Ad Hoc Transfer Module Setup](image)

   Welcome to the Secure Ad Hoc Transfer module Setup/Maintenance program. This program lets you modify the current installation. Click one of the options below:

   - **Modify**: Click Modify if you have installed this version as a Trial and now want to install the Full version.
   - **Repair**: Click Repair if you are upgrading from a previous version.
   - **Remove**: Click Remove if you want to remove Secure Ad Hoc Transfer.

2. Click on one of the following options, then click Next:

   - **Modify** - Click Modify if you have installed this version as a Trial and now want to install the Full version.
   - **Repair** - Click Repair if you are upgrading from a previous version.
   - **Remove** - Click Remove if you want to remove Secure Ad Hoc Transfer.

3. Follow the prompts to complete installation or removal.

To restart IIS

1. Click Start > Run.

2. In the Run dialog box, type `iisreset`, then press ENTER.

   A command prompt appears, IIS is reset, and then the screen closes.

**CONFIGURING SECURE AD HOC TRANSFER**

After installation of the Secure Ad Hoc Transfer (SAT) module is complete, the help file and the Web interface appear. If the Web interface does not display the SAT e-mail form, refer to Troubleshooting Errors in the Secure Ad Hoc Transfer Module.

After the installation of the SAT module is complete, a few additional steps may be necessary:

- Verify that the Microsoft IIS settings are configured correctly.
- Enable automatic notification of uploads and user cleanup events in EFT Server Enterprise. (Not available in EFT Server basic edition.)
Configure your SMTP server to allow the computer on which the SAT module is installed to relay. Refer to the following Web links for details:

- [How to troubleshoot mail relay issues in Exchange Server 2003 and in Exchange 2000 Server](http://support.microsoft.com/default.aspx?scid=kb;en-us;895853) (Microsoft KB article ID 895853)

A few other configuration options you may want to consider:

- **Customize the SAT module Web interface** - The Web e-mail interface, the SendMail form, is designed with default colors, background, and banner image. You can easily brand the SendMail form with your company logo and/or colors.

- To configure settings such as whether to use Single-Click authentication, refer to [Secure Ad Hoc Transfer's Configuration File](http://www.globalscape.com/eft/adhoc.chm) for details of editing the configuration file (web.config).

- **Using the PCI Module with the Secure Ad Hoc Transfer Module** - If you are using the HS module and the SAT module with EFT Server, you should have created a separate, non-PCI DSS Site that is used only for the SAT module. Or you can disable the features that are not compatible (e.g., administrator password expiration and forced reset), but that would take the Site out of compliance with the PCI DSS.

- **Enforcing Strong (Complex) Passwords** - If your Site’s complex password settings require more than 20 characters, you must configure the [EFTAdHoc Settings Template](http://www.globalscape.com/eft/sat_history.aspx) to override the Site’s password settings so that complex passwords for SAT temporary users contain fewer than 20 characters.

- **Sending Large Files** - If you expect to transfer large files, e.g., 1 GB or larger, we strongly recommend that you install EFT Server on the same computer as IIS and edit settings in the [SAT configuration file](http://www.globalscape.com/eft/adhoc.chm).

- **Activating Secure Ad Hoc Transfer** - When you first install the Secure Ad Hoc Transfer module, you are given the choice of installing a Full or Trial version. The trial version is not time limited, but file sender operations are limited to ten per IIS session and one file at a time. Follow the instructions in [Activating Secure Ad Hoc Transfer](http://www.globalscape.com/eft/adhoc.chm) to activate the full version.

The help file, **adhoc.chm**, can be found in the SAT installation folder (e.g., C:\inetpub\EFTAdHoc) and on the EFT Server computer in the EFT Server installation folder (e.g., C:\Program Files\GlobalSCAPE\EFT Server Enterprise). For the release notes, refer to **notes.txt** in the EFT Server installation folder or the GlobalSCAPE support page [http://www.globalscape.com/eft/sat_history.aspx](http://www.globalscape.com/eft/sat_history.aspx).
The Web e-mail interface, the SendMail form, is designed with default colors, background, and banner image. You can easily brand the SendMail form with your company logo and/or colors.

To customize the look and feel, you must edit the CSS files located in the Secure Ad Hoc Transfer module installation folder (by default, C:\inetpub\EFTAdHoc\App_Themes).

You should make a backup copy of the style sheets (CSS), skin, templates (TLT), and configuration files before you edit them. The procedures below describe how to edit elements in Main.css and default.skin. The following files are used to define the look and feel of Secure Ad Hoc Transfer:

- **AddressBook.css** – address book modal popup
- **default.skin** – .NET theme file. Can be modified to change button and banner images
- **Error.css** – error modal popup style
- **Main.css** – main script content
- **Menu.css** – used for the navigation menu
- **thickbox.css** – used for popup effects
- **web.config** - contains the e-mail notification image

### BACKGROUND COLOR

The default color behind the SendMail form is light gray. You can change the background color, which is defined in Main.css.

To change the background color

- In **Main.css**, modify the body style. For example, change:

  ```
  .Background {background-color: #F7F7F7;} /* light gray */
  ```

  To

  ```
  .Background {background-color: #FFFFFF;} /* white */
  ```
The space in which the banner image appears is called the *header*. You can change the dimensions of the header, which are 320 pixels by 63 pixels, in *main.css* to suit the size of your banner image.

**To change the size of the header image**

- In *Main.css*, modify `Header_LogoStyle`. For example, change:

  ```css
  .Header_LogoStyle {
    width: 320px;
    height: 63px;
  } /* globalscape logo image size */
  ``

  To

  ```css
  .Header_LogoStyle {
    width: 200px;
    height: 50px;
  } /* your logo image size */
  ``

**Banner Background Style**

The banner background, defined in *Main.css*, is a 1 pixel wide and 63 pixels tall blue gradient that is an expandable background for the banner image, `banner-adhoc.png`. (See *Banner Image*, below.)

**To modify the banner background style**

- In *Main.css*, modify `HeaderLogo_BackgroundStyle`. For example, change

  ```css
  .HeaderLogo_BackgroundStyle {
    background-color: #6AA6E3;
    background-image: url(images/banner-background.png);
  }
  ``

  To

  ```css
  .HeaderLogo_BackgroundStyle {
    background-color: #000000;
  } /* solid black color background */
  ``

**Banner Image**

The GlobalSCAPE banner image is defined in *default.skin*. You can replace the default banner image with your own.

**To modify the banner image**

- In *default.skin*, modify the header logo image. For example, change:

  ```xml
  <asp:Image SkinID="Header_Logo" runat="server" ImageUrl="/App_Themes/DarkGray/images/banner-adhoc.png" CssClass="Header_LogoStyle" />
  ``

  To

  ```xml
  <asp:Image SkinID="Header_Logo" runat="server" ImageUrl="/App_Themes/DarkGray/images/your-image-here.jpg" CssClass="Header_LogoStyle" />
  ```
CUSTOMIZING THE NOTIFICATION E-MAIL

You can customize the look of the e-mail that the Server sends to recipients when a file is uploaded to the Server. The logo used for notification e-mails is `email_logo.gif`, installed by default in `C:\inetpub\EFTAdHoc\App_Themes\Images\`. You can remove the logo from the e-mail or replace it with your own.

To change this logo image

1. Copy the new logo image into the folder `C:\inetpub\EFTAdHoc\App_Themes\Images\`.
2. In `web.config`, modify the variable `ImageLogoFileName` with the new file name. For example, change:
   ```xml
   <add key="ImageLogoFileName" value="email_logo.gif" />
   ```
   To
   ```xml
   <add key="ImageLogoFileName" value="your-image-here.jpg" />
   ```

To remove the logo image

- In `web.config`, set the variable `RemoveImageLogoAttachment` to True. Change:
  ```xml
  <add key="RemoveImageLogoAttachment" value="False" />
  ```
  To
  ```xml
  <add key="RemoveImageLogoAttachment" value="True"/>
  ```
CONFIGURING TEMPORARY USER ACCOUNT EXPIRATION

By default, accounts that are created when you send a file to a recipient that is not defined in EFT Server, the account expires after 7 days. You can configure the number of days after which the account is to expire or configure the account to not expire.

To configure temporary account expiration

- In web.config or in the IIS properties, set the variable ExpiryDays to the number of days after which the account is to expire or 0 (zero) if you do not want the account to expire.

  You can still expire or disable the account later in the EFT Server administrator interface.

Refer to Secure Ad Hoc Transfer's Configuration File for details of editing the configuration file.

EDITING THE CONFIGURATION FILE (WEB.CONFIG)

Secure Ad Hoc Transfer uses a configuration file, web.config, located by default in C:\inetpub\EFTAdHoc. The installer captures and records all necessary values; however, you can manually change those settings in the IIS Manager. You can manually edit web.config (e.g., in a text editor or Visual Studio), but you have to be very careful with your edits so as not to introduce errors in the formatting of the file. You should create a backup copy of the file before editing.

To open the EFTAdHoc Properties

1. Open the Internet Information Services manager. (Click Start, Programs > Administrative Tools > Internet Information Services (IIS) Manager.)
2. Expand the Web Sites node, then expand the Default Web Site node.
3. Right-click EFTAdHoc, then click Properties.
4. In the Properties dialog box, click the ASP.NET tab. (If the Properties dialog box does not have an ASP.NET tab, refer to AdHoc Properties Missing ASP.NET Tab.)
5. Click **Edit Configuration**. The **ASP.NET Configuration Settings** dialog box appears.

![ASP.NET Configuration Settings Dialog Box](image)

6. Click the **General** tab. The settings in the **web.config** file for the SAT Module appear in the **Application settings** area.

7. To change a value, click it, then click **Edit**. In the **Edit/Add Application Settings** dialog box, type the new value, then click **OK**. Do not remove any of the keys.

8. After you have viewed/edited the configuration, click **OK** to close the dialog boxes, then, in the IIS Manager, click **File > Close**. It is not necessary to restart the service or reboot.

---

*Any changes you make to the file must be replicated on any computer running EFT Server.*

### EFT Server Configuration

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Default/Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>EFTServerIPAddress</td>
<td>EFT Server Admin GUI IP address</td>
<td>IP Address or localhost</td>
</tr>
<tr>
<td>EFTServerPort</td>
<td>EFT Server Admin GUI port</td>
<td>1100</td>
</tr>
<tr>
<td>EFTAdminUsername</td>
<td>EFT Server Admin GUI username</td>
<td>no default</td>
</tr>
<tr>
<td>EFTAdminPassword</td>
<td>EFT Server Admin GUI password (use <code>encode.htm</code> to obfuscate)</td>
<td>no default</td>
</tr>
<tr>
<td>EFTSite</td>
<td>EFT Server Site name under which SAT module Settings Template will be created</td>
<td>MySite</td>
</tr>
<tr>
<td>SettingsLevel</td>
<td>EFT Server Settings Template under which SAT module users will be created</td>
<td>EFTAdHoc</td>
</tr>
</tbody>
</table>
## Global Configuration Variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Default / Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>URLPattern</td>
<td>URL pattern that should be used in the outgoing e-mails. When the recipient receives the e-mail notification, they are told to click this link to pick up the attachment.</td>
<td><a href="https://server1.com:443/">https://server1.com:443/</a></td>
</tr>
<tr>
<td>ExpiryDays</td>
<td>Number of days before SAT module user accounts expire.</td>
<td>7</td>
</tr>
<tr>
<td>TempUserNameLength</td>
<td>SAT Module username length</td>
<td>10</td>
</tr>
<tr>
<td>LogPath</td>
<td>Path where the verbose debugging log file will be created (if enabled)</td>
<td><code>c:\inetpub\wwwroot\EFTAdhoc\temp\logs</code></td>
</tr>
<tr>
<td>UseLogFiles</td>
<td>True (1) = the application will log errors, configuration errors, and event information False (0) = the application will not log any debug information</td>
<td>True</td>
</tr>
</tbody>
</table>

*File path must be explicitly defined and the IUSR_<computername> must have write permission to this path.*

*If authentication is enabled for SAT then "Authenticated Users“ must have write permission to this path.*
## Troubleshooting Errors in the Secure Ad Hoc Transfer Module

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Default / Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogLevel</td>
<td>Log level for debugging. Where 0 is the least log output and 5 is the greatest amount of log output. 0 = debug - None of any log messages are logged. 1 = error - Only exceptions or errors are logged. 2 = events - Logs information related to each event (or action) after it is executed, such as &quot;Email Sent,&quot; &quot;EFT Server Connected,&quot; &quot;File Uploaded.&quot; 3 = info - Logs messages that contain additional information such as parameters, variables, or configuration. 4 = verbose - Logs actions that are about to execute and when the action has been executed. e.g., &quot;Connecting EFT&quot; then the connection occurs and a &quot;EFT Connected&quot; message is logged. Another example &quot;Sending Email&quot; and after the e-mail is sent &quot;Email Sent.&quot; When you specify a logging level, the system collects messages for that level and all the levels below it. That is, level 2 includes level 1, level 3 includes level 2 and level 1, and so on.</td>
<td>1 is the default; range is 0-4</td>
</tr>
<tr>
<td>TempFolder</td>
<td>Temporary folder for file uploads on IIS server</td>
<td>c:\inetpub\wwwroot\EFTAdhoc\temp\TempFolder</td>
</tr>
<tr>
<td>LockFromField</td>
<td>Enable or disable users from modifying the &quot;From&quot; field text box, specifically used when from is populated from Active Directory.</td>
<td>False</td>
</tr>
</tbody>
</table>
## Mail Content Configuration

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Default / Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>EmailTemplateFormat</td>
<td>E-mail template format, Plain Text or HTML, to be used when the system sends an e-mail. The templates used depend on this variable setting. (e.g., UsernamePasswordTemplate.tlt or UsernamePasswordTemplateTextPlain.tlt)</td>
<td>0 = HTML 1 = Plain Text</td>
</tr>
<tr>
<td>EmailBehavior</td>
<td>SAT default e-mail behavior allowing username and password to be send in separate e-mails or single-click authentication. Single-Click authentication allows the user to automatically log into the Web Transfer Client using an authentication link.</td>
<td>0 or 1 = Username and Password in one e-mail to recipient 2 = Username and Password in separate e-mails to recipient 3 = Username and Password in separate e-mails to sender 4 = Username to recipient and Password to sender 5 = Single-Click Authentication</td>
</tr>
<tr>
<td>SystemEmail</td>
<td>E-mail address configured when SAT was installed.</td>
<td>no default</td>
</tr>
<tr>
<td>UsernamePasswordTemplate</td>
<td>E-mail template containing the username and password as one e-mail message. Used when EmailBehavior is set to 1.</td>
<td>UsernamePasswordMessage.tlt</td>
</tr>
<tr>
<td>SingleClickAuthMessageTemplate</td>
<td>E-mail template containing the username and password as one e-mail message. Used when EmailBehavior is set to 5.</td>
<td>SingleClickAuthenticationMessage.tlt</td>
</tr>
<tr>
<td>UsernameMessageTemplate</td>
<td>E-mail template containing the username and password as one e-mail message. Used when EmailBehavior is set to 2-4.</td>
<td>UsernameMessage.txt</td>
</tr>
<tr>
<td>PasswordMessageTemplate</td>
<td>E-mail template containing the username and password as one e-mail message. Used when EmailBehavior is set to 2-4.</td>
<td>PasswordMessage.txt</td>
</tr>
<tr>
<td>UploadNotificationTemplate</td>
<td>E-mail template used for upload notification e-mails from SendUploadNotification.wsf script.</td>
<td>SendUploadNotificationMessage.txt</td>
</tr>
<tr>
<td>UsernamePasswordTemplateTextPlain</td>
<td>Plain Text E-mail template containing the username and password as one e-mail message. Used when EmailBehavior is set to 1</td>
<td>UsernamePasswordMessageTextPlain.tlt</td>
</tr>
</tbody>
</table>
## Troubleshooting Errors in the Secure Ad Hoc Transfer Module

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Default / Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>SingleClickAuthMessageTemplateTextPlain</td>
<td>Plain Text E-mail template containing the username and password as one e-mail message. Used when EmailBehavior is set to 5.</td>
<td>SingleClickAuthenticationMessageTextPlain.tlt</td>
</tr>
<tr>
<td>UsernameMessageTemplateTextPlain</td>
<td>Plain Text E-mail template containing the username and password as one e-mail message. Used when EmailBehavior is set to 2-4.</td>
<td>UsernameMessageTextPlain.tlt</td>
</tr>
<tr>
<td>PasswordMessageTemplateTextPlain</td>
<td>Plain Text E-mail template containing the username and password as one e-mail message. Used when EmailBehavior is set to 2-4.</td>
<td>PasswordMessageTextPlain.tlt</td>
</tr>
<tr>
<td>UploadNotificationTemplateTextPlain</td>
<td>Plain Text E-mail template used for upload notification e-mails from SendUploadNotification.wsf script.</td>
<td>SendUploadNotificationMessageTextPlain.tlt</td>
</tr>
<tr>
<td>ImageLogo</td>
<td>Image logo used in the e-mail templates (not used in the Plain Text templates)</td>
<td>email_logo.gif</td>
</tr>
<tr>
<td>RemoveImageLogoAttachment</td>
<td>Removes the logo image attachment from all e-mail messages if set to True.</td>
<td>False</td>
</tr>
</tbody>
</table>

### SMTP Configuration

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Default / Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTPServer</td>
<td>SMTP server hostname or IP address through which notifications will be sent</td>
<td>no default</td>
</tr>
<tr>
<td>SMTPDomain</td>
<td>SMTP server hostname or IP address for sending notification mails, used only with cdoNTLM SMTP Authentication.</td>
<td>Blank if SMTPAuthenticate is 0.</td>
</tr>
<tr>
<td>SMPTPServerPort</td>
<td>Port used by SAT module for SMTP communication</td>
<td>25</td>
</tr>
<tr>
<td>SMTPAuthenticate</td>
<td>SMTP server authentication mode. cdoAnonymous=0 cdoBasic=1 cdoNTLM=2</td>
<td>0</td>
</tr>
<tr>
<td>SendUserName</td>
<td>SMTP username for authentication (when required)</td>
<td>no default</td>
</tr>
<tr>
<td>SendPassword</td>
<td>SMTP password used for authentication (when required)</td>
<td>no default</td>
</tr>
</tbody>
</table>
### Smart E-Mail Options

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Default / Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>UseSmartEmailTextBoxes</td>
<td>When set to true, enables smart e-mail text boxes. SAT will identify users based on first and last name for all Sites if the full name and e-mail fields are populated.</td>
<td>False</td>
</tr>
<tr>
<td>CacheDurationEFTUsersMins</td>
<td>The duration in minutes before caching users used for Smart E-mail text boxes.</td>
<td>60</td>
</tr>
</tbody>
</table>

### E-Mail Filtering Options

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Default / Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnableEmailFiltering</td>
<td>When set to true enables white/blacklist filtering options to destination domains for To/Cc/Bcc e-mail addresses.</td>
<td>False</td>
</tr>
<tr>
<td>WhiteListDestinationDomain</td>
<td>Specifies the allowed destination domain when BlackListDestinationDomain is set to *. Use comma to separate list of domains.</td>
<td>* (asterisk)</td>
</tr>
<tr>
<td></td>
<td>Example: WhiteListDestinationDomain value=&quot;globalscape.com&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BlackListDestinationDomain value=&quot;*&quot;</td>
<td></td>
</tr>
<tr>
<td>BlackListDestinationDomain</td>
<td>Specifies the restricted destination domains when WhiteListDestinationDomain is set to *. Use comma to separate list of domains.</td>
<td>blank</td>
</tr>
<tr>
<td></td>
<td>Example: WhiteListDestinationDomain value=&quot;*&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BlackListDestinationDomain value=&quot;globalscape.com,domaínname.com&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Allow all e-mails except to globalscape.com or domainname.com domains.)</td>
<td></td>
</tr>
</tbody>
</table>
### SAT Module EFT Server Communication Configuration

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Default / Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>UploadProtocol</td>
<td>Internal protocol used for transferring from SAT module storage to EFT Server</td>
<td>(See <a href="#">Using the PCI Module with the Secure Ad Hoc Transfer Module</a> for details of this setting with HS-enabled Sites.)</td>
</tr>
<tr>
<td></td>
<td>-1 = Local File Copy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0 = FTP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 = FTP Implicit SSL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2 = FTP Explicit SSL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3 = SFTP2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4 = HTTP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5 = HTTPS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6 = SOCKS4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7 = SOCKS5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8 = FTP AUTH TLS</td>
<td></td>
</tr>
<tr>
<td>UploadPort</td>
<td>The port number to use in the upload process. This value is not necessary if you use “Local File Copy” (-1) for UploadProtocol.</td>
<td>443</td>
</tr>
</tbody>
</table>

### Script Configuration

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Default / Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>WaitForUploadsDurationSec</td>
<td>Used for the Send Upload Notification script. Duration in seconds to wait for uploaded files prior to sending e-mail notification. The frequency of the timer event rule that is monitoring home folders affects the delay between uploaded files and the notification message.</td>
<td>30</td>
</tr>
</tbody>
</table>

### Active Directory Server Configuration

You must specify an alternate form of authentication in IIS for the Active Directory Server Configuration to function.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Default / Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>UseADExtensions</td>
<td>This setting enables or disables the Active Directory Server Configuration settings defined below.</td>
<td>False</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
<td>Default / Range</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>AD-AuthorizedGroupListName</td>
<td>Defines the Active Directory group names used to specify which groups have access to SAT.</td>
<td>*</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> A comma is used to separate a list of group names or * will allow all groups access to SAT.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Group List Examples:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;GROUP-01, GROUP-02, GROUP-03&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;*&quot;</td>
<td></td>
</tr>
<tr>
<td>AD-SetFromFieldWithEmail</td>
<td>If the value is set to True, the From e-mail address will obtain the current logged user’s e-mail address from Active Directory.</td>
<td>True</td>
</tr>
<tr>
<td>Path</td>
<td>Path utilized in LDAP query including Host Name, Port, and BaseDN</td>
<td>no default</td>
</tr>
<tr>
<td></td>
<td>Path Examples:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;LDAP://RootDSE&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;LDAP://DOMAIN:389/OU=XXXXX,DC=XXXX,DC=XXXX&quot;</td>
<td></td>
</tr>
<tr>
<td>SearchFilter</td>
<td>LDAP search filter configuration to retrieve user e-mail address. %USER.LOGIN% will be replaced with the actual login name for the current SAT user.</td>
<td>(&amp;(objectClass=person)(</td>
</tr>
<tr>
<td>Attributes</td>
<td>The set of attributes to be retrieved from the query.</td>
<td>cn,sAMAccountName, userPrincipalName,mail,displayName,sn</td>
</tr>
<tr>
<td>Scope</td>
<td>Search Scope:</td>
<td>Subtree</td>
</tr>
<tr>
<td></td>
<td><strong>Base</strong> = Limits the search to the base object. The result contains one object at most.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>OneLevel</strong> = Searches the immediate child objects of the base object, excluding the base object.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Subtree</strong> = Searches the whole subtree, including the base object and all its child objects.</td>
<td></td>
</tr>
</tbody>
</table>
### Troubleshooting Errors in the Secure Ad Hoc Transfer Module

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Default / Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>UseConfiguredDomainAccount</td>
<td>The authentication method used to connect to Active Directory.</td>
<td>Secure</td>
</tr>
<tr>
<td></td>
<td><strong>None</strong> = Equates to zero, which means to use basic authentication (simple bind) in the LDAP provider.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Anonymous</strong> = No authentication is performed</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Delegation</strong> = Enables Active Directory Services Interface (ADSI) to delegate the user’s security context, which is necessary for moving objects across domains.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Secure</strong> = Requests secure authentication.</td>
<td></td>
</tr>
<tr>
<td><strong>NOTE:</strong> If the UseConfiguredDomainAccount = &quot;&quot; then UseConfiguredDomainAccount is set as &quot;AuthenticationTypes.None&quot; by default.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DomainAdminUser</td>
<td>This setting is required when the UseConfiguredDomainAccount is set to Secure. The user name of an account that has the ability to query Active Directory.</td>
<td>no default</td>
</tr>
<tr>
<td></td>
<td>User Name Examples: &quot;username&quot; &quot;domain\username&quot;</td>
<td></td>
</tr>
<tr>
<td>DomainAdminPass</td>
<td>This setting is required when the UseConfiguredDomainAccount is set to Secure. The base64 encoded password of the account that has the ability to query Active Directory. (use encode.htm to obfuscate)</td>
<td>no default</td>
</tr>
<tr>
<td>SenderEmailDisplayAttribute</td>
<td>Active Directory attribute name used to retrieve the From e-mail address</td>
<td>mail</td>
</tr>
</tbody>
</table>
IIS AUTHENTICATION

The Secure Ad Hoc Transfer (SAT) module selects anonymous access by default for the EFTAdhoc virtual directory, but alternate authentication methods are also supported. If an alternate form of authentication is defined, the Authenticated Users group in IIS must be granted full permission to the EFTAdhoc folder.

SAT can be configured to allow access by Active Directory group membership or to populate the From address with the current user’s e-mail address from Active Directory. In order for these settings to function, an alternate form of authentication such as Basic authentication or Integrated Windows authentication must be enabled in the Authentication Methods dialog box. Also, ensure that the Enable anonymous access check box is not selected.

CREATING A BASE64-ENCODED PASSWORD

For communication between IIS and EFT Server, the installer uses the EFT Server administrator password, which is stored in the configuration file (located by default in C:\Inetpub\EFTAdHoc) using simple obfuscation. It is highly recommended that you use the delegated administration feature of EFT Server to create a new administrative account that can be used by the Secure Ad Hoc Transfer module. This isolates the username/password for the Web application, independent of EFT Administrator. Also, if the EFT Server has multiple Sites, you should grant access to this Secure Ad Hoc Transfer application only to the Site that is used by this application.

After the installer has completed successfully, set up a new administrator account in EFT Server, then follow the procedure below to create a base64-encoded password.
To create a base64-encoded password

1. In your Web browser, type the URL for the SAT send page with encode.htm at the end of the address. For example, type:
   
   http://localhost/EFTAdHoc/encode.htm

   The GlobalSCAPE WebAdmin Base64 Encode Utility appears.

2. In Enter password and Confirm password boxes, type the administrator password, then click Encode to create the obfuscated version of the password.

3. In the configuration file located in the Secure Ad Hoc Transfer installation folder, edit the EFTAdminPassword value, replacing it with the obfuscated password you just created. Also, replace EFTAdminUsername with the new administrator username you just created.

SPECIFYING VIRTUAL FOLDERS FOR AD HOC USERS

If you would like to store Ad Hoc users' folders on a remote computer, you can configure that in EFT Server's Virtual File System. Similar to a shortcut, you can point a Virtual Folder to a physical path on the same computer or on a remote computer, but the computer on which Secure Ad Hoc Transfer and IIS are installed must have permission to write to the folder.

To specify Virtual Folders for Ad Hoc users

1. Create the shared folder on the computer on which you want to store Ad Hoc users' home folders.

2. Ensure that Secure Ad Hoc Transfer and IIS have read and write permission on the folder.

3. In EFT Administrator, connect to the Server, then click the VFS tab.

4. Right-click the Site tree, then click New Virtual Folder. The New Virtual Folder dialog box appears.
5. In the **Alias** box, type any name. For example, type adhoc2.

6. In the **Target** box, type the physical path to the location. For example, type \10.1.2.3\adhoc2

7. Click **OK**.

8. Click the **Server** tab, then click the **Adhoc** node.

9. On the **Main** tab, in the **Home folder** box, type the Virtual Folder name.

10. Click **Apply** to save the changes on the Server.

Now when a file is sent, the Ad Hoc user's home folder is created at the location you specified for the Virtual Folder.

**ADDING BLACKLIST AND WHITELIST DOMAINS**

You can configure Secure Ad Hoc Transfer to block (Blacklist) or allow (Whitelist) only specific domains. For example, if you do not want users to send files to certain e-mail accounts, you would add that domain to the blacklist.

**To configure the blacklist and whitelist**

1. Open the **Internet Information Services** manager. (Click **Start**, **Programs** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.)

2. Expand the **Web Sites** node, then expand the **Default Web Site** node.

3. Right-click **EFTAdHoc**, then click **Properties**.

4. In the **Properties** dialog box, click the **ASP.NET** tab. (If the **Properties** dialog box does not have an **ASP.NET** tab, refer to **AdHoc Properties Missing ASP.NET Tab**.)

5. Click **Edit Configuration**. The **ASP.NET Configuration Settings** dialog box appears

6. Click the **General** tab. The settings in the **web.config** file for the SAT Module appear in the **Application settings** area.

7. Scroll to **BlacklistDestinationDomain**, click it, then click **Edit**.

8. In the **Edit/Add Application Settings** dialog box, type the domain or string to block from being used in the **To**, **Cc**, or **Bcc** boxes in the SendMail form, then click **OK**. Separate multiple domains with commas.

9. Scroll to **WhitelistDestinationDomain**, click it, then click **Edit**. By default all domains (*) are allowed.

10. In the **Edit/Add Application Settings** dialog box, type the domain or string to allow in the **To**, **Cc**, or **Bcc** boxes in the SendMail form, then click **OK**. Separate multiple domains with commas.

11. Click **OK** to close the **ASP.NET Configuration Settings** dialog box.
SINGLE-CLICK AUTHENTICATION

You can configure the Secure Ad Hoc Transfer notification e-mail to include a hyperlink to log the recipient in to the Web Transfer Client automatically to download the files that were sent.

A variable in the web.config file, EmailBehavior, allows you to specify the way in which recipients receive login information when files are uploaded to the Server. The value of the variable determines the behavior:

0 or 1 = Username and Password in one e-mail to recipient
2 = Username and Password in separate e-mails to recipient
3 = Username and Password in separate e-mails to sender
4 = Username to recipient and Password to sender
5 = Single-Click Authentication

You can also configure the logo in the message to either remove it or replace it with your own. The sender provides the text in the body of the e-mail when it is sent.

USING SAT WITH ACTIVE DIRECTORY

The Secure AD Hoc Transfer (SAT) module can work with Active Directory (AD) authentication.

To make AD work with SAT, edit the following configuration:

- Edit the AD-specific settings in the SAT module's web.config file. The Active Directory Server Configuration section of the online help topic Editing the Configuration File details each of the defined settings in the web.config file.
Secure Ad Hoc Transfer Module for EFT Server v6.1

- Specify an alternate form of authentication in IIS. The IIS Authentication section of the online help topic Editing the Configuration File describes how to specify an alternate form of authentication, such as Basic authentication or Integrated Windows authentication, which must be enabled in the Authentication Methods dialog box. Ensure that the Enable anonymous access check box is not selected.

- If an alternate form of authentication is defined, the Authenticated Users group in IIS must be granted full permission to the EFTAdhoc folder (e.g., C:\inetpub\EFTAdHoc).

For example, to populate the Secure Ad Hoc web page and lock the From field, you would edit the following variables:

```
"UseADExtensions" value="True"
"AD-SetFromFieldWithEmail" value="True"
"SearchFilter" value="(&(objectClass=person) (|(sAMAccountName=%USER.LOGIN%)(userPrincipalName= %USER.LOGIN%)(mail=%USER.LOGIN%)))"
"Attributes" value="cn,sAMAccountName,userPrincipalName,mail,displayName,sn"
"Scope" value="Subtree"
"UseConfiguredDomainAccount" value="Secure"
"SenderEmailDisplayAttribute" value="mail"
"LockFromField"="True"
```

(LockFromField is one of the Global variables)

Refer to Editing the Configuration File for more variables and information about editing the SAT configuration file.

RECEIVING NOTIFICATIONS WHEN RECIPIENTS UPLOAD FILES

EFT Server will populate the EFTAdHoc User Setting Template with the temporary user accounts as they are created.

If you have Event Rules to trigger on account creation or password change, those Rules are triggered when the temporary account is created.

The procedure below is for EFT Server Enterprise administrators only. This procedure is performed on the EFT Server Enterprise computer in the Administrator interface. EFT Server basic edition has no Timer Event Rule functionality. You cannot configure EFT Server basic edition to alert you on upload notifications of SAT users. If you send a SAT e-mail to a user, then that user uploads something back to you, there is no way to configure the “return upload” notification to let you know your temporary user has uploaded something for you to pick up. This functionality relies on a Timer Rule that is only available with EFT Server Enterprise.

Nor can you configure EFT Server basic edition to automatically remove expired SAT temporary accounts. The removal of the temporary accounts is triggered by the Timer Event running a script. The script is still available in EFT Server basic edition and you can run it manually to clean up expired accounts, but there is no Timer Event to have this happen automatically. You could also run the script with the Log Rotated Event so that the script is run daily, weekly, or monthly, depending on how often the log is rotated. (For more information about logs, refer to the EFT Server help topic.)

The Secure Ad Hoc Transfer (SAT) module default installation handles the process of notifying your recipients when a file is sent. In addition, temporary accounts are disabled automatically one week after account creation.
To remove expired temporary accounts from EFT Server (including their home folder and any files contained within) automatically, and to receive notifications for files uploaded by recipients, you must configure EFT Server to do so, as described below.

The SendUploadNotification.wsf script contains two jobs, File Uploaded and Scheduler (Timer), that work together to send a notification mail to the account creator (the "From" e-mail address) whenever file(s) are uploaded into the temporary account. The Scheduler (Timer) job creates a hidden temporary file within the temp user’s home folder indicating an upload is in progress. The Scheduler (Timer) job periodically queries the home folders for accounts and, if a temp file is found, a notification is sent to the account owner. The script uses the web.config for the SMTP configuration and the “WaitForUploadsDurationSecs” variable specifying the number of seconds to wait for uploaded files prior to sending e-mail notification. The script also requires the SendUploadNotificationMessage.tlt template located in the Templates directory.

The system is configured to notify the original sender any time the external recipient performs an upload. This is done by setting up the File Uploaded and the Scheduler (Timer) rules on EFT Server. The frequency of the Scheduler (Timer) rule governs how often the upload notifications are sent. You can edit the SendUploadNotificationMessage template file to be more descriptive. (This file is on the EFT Server computer, not the IIS computer.)

To receive notifications when recipients upload files

Part 1: Configure the “Send Upload Notification to Sender - On Upload” event rule

1. If EFT Server and IIS are installed on separate computers, copy the EFTAdHoc folder (by default, C:\Inetpub\wwwroot\EFTAdHoc\) and its contents to the EFT Server computer.

2. Open EFT Administrator and create a new custom command for cscript.exe (a Windows system file usually located at c:\windows\system32\cscript.exe) as illustrated below.

3. In the left pane, click Event Rules, then, in the right pane, click New. The Create New Rule dialog box appears.

4. In the Event Rule Name box, type a name for the rule. For example, type Send Upload Notification to Sender.

5. In the Description box, type a comment. (Optional)

6. In the Select event trigger list, click File Uploaded.

7. Click Create. The Event Rules tab appears.
8. In the **Conditions** box, scroll to **Connection Conditions**, and double-click **If Remote IP does match [ip mask]**. The condition appears in the **Rule** pane.

9. In the **Conditions** box, scroll to **User Conditions**, and double-click **If Settings Template does equal**. The condition is added next to the first condition, on the same line.

10. In the condition **If Remote IP does match [ip mask]**, click **does** once to change it to **does not**.

    **If you are using the EFT Secure Ad Hoc Transfer Module, and if EFT Server and IIS are installed on the same computer, when creating the Event Rule for Upload Notifications, create an additional Condition for REMOTE IP does not match 127.0.0.1.**

    The Rule's Conditions should read:

    If Settings Template is EFTAdHoc
    AND If remote ip does not match <ip address of IIS server>
    AND If remote ip does not match 127.0.0.1

    The second Condition should **not** be added if EFT Server and IIS are **not** installed on the same computer.

11. Click **[ip mask]**. The **Edit Value** dialog box appears.

12. Type the IP address for the IIS host; click **OK**.

13. In the condition **If Settings Template does equal to [Settings Template]**, click **[Setting Template]**. The **Select Settings Template** dialog box appears.

14. Click the down arrow to click the Settings Template used by Secure Ad Hoc Transfer (by default, **EFTAdHoc**), then click **OK**.

15. In the **Actions** box, double-click **Execute command in folder**. The new action appears UNDER the new compound condition that you just created and is indented, as shown below.
Troubleshooting Errors in the Secure Ad Hoc Transfer Module

16. In the Action **Execute command select in folder 'c:\',** click select. The **Custom Command** dialog box appears.

![Custom Command dialog box](image)

17. In the **Select command** drop-down list, click the name that you gave the cscript command.

18. In the **Specify command parameters** box, type or paste the following text:

   SendUploadNotification.wsf //JOB:ON_UPLOAD %USER.LOGIN% %FS.VIRTUAL_PATH%

19. In the **Specify command working folder** box, click the directory in which the script exists. The script is in the **Scripts** subdirectory of the Secure Ad Hoc Transfer installation folder if IIS and EFT Server are on the same system (C:\inetpub\wwwroot\EFTAdHoc\Scripts) or the **Scripts** subdirectory of the folder you copied in step 1.

20. Click **OK** to close the **Custom Command** dialog box.

21. Click **Apply** to save the changes on EFT Server.

22. Continue to Part 2, below.

**Part 2: Configure the "Send Upload Notification to Sender - On Timer" Event Rule**

1. Create a new Rule using the **Scheduler (Timer) Event**.

2. In the **Actions** box, double-click **Execute command in folder** to add it to the Rule pane.

   ![Execute command in folder](image)

3. In the Rule pane, in the Execute command Action, click select. The **Custom Command** dialog box appears.

   ![Custom Command dialog box](image)
4. In the Select command drop-down list, click the name that you gave the cscript command in Part 1.

5. In the Specify command parameters box, type or paste the following text:
   
   SendUploadNotification.wsf //JOB:ON_TIMER

6. In the Specify command working folder box, click the directory in which the script
   SendUploadNotification.wsf exists. (In the Scripts subdirectory of the Secure Ad Hoc Transfer installation
   folder if IIS and EFT Server are on the same system, C:\inetpub\wwwroot\EFTAdHoc\Scripts, or the
   Scripts subdirectory of the folder you copied from the IIS computer.)

7. Click OK to save the Command.

8. Click Apply to save the changes on EFT Server.

Next, Create a Timer Rule to Remove Temporary Expired Accounts.

CREATING A TIMER RULE TO REMOVE TEMPORARY EXPIRED ACCOUNTS

(Only available in EFT Server Enterprise) To remove expired temporary accounts from EFT Server Enterprise
automatically (including their home folder and any files contained within), you must create a custom Command to
execute a script and then execute the Command as an Action in a Timer Event Rule, as described below.

To create a timer rule to remove temporary expired accounts:

1. Create a Custom Command to use cscript (in C:\Windows\system32\cscript.exe).

2. Create a new Rule using the Scheduler (Timer) Event.

3. Click repeat each 01:00:00. The Timer Event dialog box appears.

4. Specify the time, date, and frequency (recurrence pattern) the Rule is to execute, then click OK (e.g.,
every day at 1 a.m.).

5. In the Event Rules Actions box, double-click Execute command in folder to add it to the Rule pane.

6. In the Execute command select in folder 'c:\' Action, click select. The Custom Command dialog box
appears.
7. In the **Select command** drop-down list, click the name that you gave the Command in step 1.

8. In the **Specify Command Parameters** box, type or paste the following text:

   ```
   EFTDeleteExpiredUsers.wsf
   ```

9. In the **Specify Command Working Folder** box, click the directory in which the script exists. (In the **Scripts** subdirectory of the Secure Ad Hoc Transfer installation folder if IIS and EFT Server are on the same system, `C:\inetpub\EFTAdHoc\Scripts` or the **Scripts** subdirectory of the folder you copied from the IIS computer.)

10. Click **OK** to close the Custom Command dialog box.

11. Click **Apply** to save the changes on EFT Server.

---

**SCHEDULER (TIMER) EVENT**

*EFT Server basic edition has no Timer Event Rule functionality. You cannot configure EFT Server basic edition to alert you on upload notifications of SAT users. If you send a SAT e-mail to a user, then that user uploads something back to you, there is no way to configure the "return upload" notification to let you know your temporary user has uploaded something for you to pick up. This functionality relies on a Timer Rule that is NOT available with EFT Server basic edition.*

(Available in EFT Server Enterprise) The Scheduler (Timer) Event allows you to execute a specified Action (e.g. send an e-mail or a report) only one time or to recur at specified intervals. For example, you could schedule the Clean Up Action to occur on July 8 at midnight, or every Monday morning, or on the last Friday of every month at 2 a.m.

A recurring Timer does not stop recurring if the Rule Actions fail; it will continue to recur as scheduled until you disable or delete the Rule. For example, suppose you want to download a file from a remote server, delete the file from the remote location after transfer, then send yourself an e-mail. If the file that you want to download is not yet in the remote directory, the Rule will fail for that particular instance of the Timer running, but it will run again at the next scheduled time (e.g., every four hours). In the case of Timer Rules, "Stop processing this rule" means "do not execute any further Actions with this Rule" (such as sending an e-mail), but it does NOT mean that the Timer will stop. For example, if you have defined the Rule to run every hour, the Timer Rule will fail when the file is not in the remote location, but the Timer Rule will run again the next hour, and the next hour, and so on, until you tell it to stop (by manually disabling it).
You can use the Event Rule to execute a script that accesses a remote server, downloads a file, deletes the source file, and then disables the Rule (through COM), but the purpose of Event Rules is to not require a script.

To define a Timer Rule to download a remote file

1. In EFT Administrator, connect to EFT Server and click the Server tab.
2. Do one of the following:
   - Right-click in the left pane, then click New Event Rule.
   - In the left pane, expand the Site you want to configure, then click Event Rules. In the right pane, click New.
   - On the main menu, click Configuration > Create New Event Rule.
   The Create New Event Rule dialog box appears:
3. In the Event Rule Name box, type a descriptive name for the Rule.
4. In the Description box, enter any notes about the rule, such as “Scheduling.” You can edit these notes later in the Comment area for the Rule.
5. In the Select event trigger box, click Scheduler (Timer) Event, then click OK. The new Rule appears in the Rule pane.
   
6. The Rule is defined by default to trigger each hour starting on the date that you create the Rule. To change the start date, start time, recurrence pattern, and/or interval, in the Rule pane, click repeat each 01:00:00. The Timer Event dialog box appears.
7. Specify the start time, start date, and recurrence pattern (frequency). The following recurrence options are available:

- **Hourly** - The timer is activated every \(<n>\) hours: \(<n>\) minutes: \(<n>\) seconds.
- **Daily** - The timer is activated every \(<n>\) days, or every weekday.
- **Weekly** - The timer recurs every \(<n>\) weeks on the weekday (Sunday - Saturday) that you specify.
- **Monthly** - The timer recurs on day \(<n>\) of every \(<n>\) month(s) or the first, second, third, fourth, or last weekday (Sunday - Saturday) that you specify of every \(<n>\) month.
- **Yearly** - The timer recurs every \(<month> <day>\) (e.g., September 30) or the first, second, third, fourth, or last weekday (Sunday - Saturday) that you specify of a specific month.
- **Once** - The timer is activated only once on the Start date and Start time that you specify.

8. Click **OK**. The changes appear in the **Rule** pane.

9. Specify the Action to occur when this Event is triggered, such as [executing a script](#).

10. Click **Run Now** to test your Rule.

    **When you create a Timer rule, the Run Now button appears at the bottom of the Rule pane. When you click Run Now, EFT Server executes any actions associated with the Event, and any Rule construction errors are identified. You cannot perform any other operations in EFT Administrator while EFT Server tests the Rule. Multiple synchronous Actions defined in the Rule, such as move, copy, or download, take longer to test than asynchronous operations such as e-mail notifications.**

11. If there are no errors, a confirmation message appears asking you to verify the expected outcome. Click **Continue** to execute the Rule or **Cancel** to refine the Rule.

12. Click **Apply** to save the changes on EFT Server.
DEFAULT TEMPLATE LOCATIONS

E-mail notifications are formatted by templates stored on the IIS server computer or the EFT Server computer.

- **Send files via SAT (stored on IIS server computer)**
  (Based on the “EmailBehavior” and “EmailTemplateFormat” settings defined in `web.config`)
  - **PasswordMessage.tlt** and **PasswordMessage.txt**
    - Physical Location: `C:\inetpub\wwwroot\EFTAdhoc\Templates`
  - **SingleClickAuthenticationMessage.tlt** and **SingleClickAuthenticationMessage.txt**
    - Physical Location: `C:\inetpub\wwwroot\EFTAdhoc\Templates\`
  - **UsernameMessage.tlt** and **UsernameMessage.txt**
    - Physical Location: `C:\inetpub\wwwroot\EFTAdhoc\Templates\`
  - **UsernamePasswordMessage.tlt** and **UsernamePasswordMessage.txt**
    - Physical Location: `C:\inetpub\wwwroot\EFTAdhoc\Templates\`

- **Upload notification via EFT Server (stored on EFT Server computer)**
  - **SendUploadNotificationMessage.tlt** and **SendUploadNotificationMessage.txt**
    - Physical Location: `C:\inetpub\EFTAdHoc\Templates\` *(or `C:\inetpub\wwwroot\EFTAdhoc\Templates\` if EFT Server and IIS are installed on the same computer)*

SPECIFYING HTML OR_plain Text E-MAIL FORMAT

In Secure Ad Hoc Transfer’s configuration file, you can specify whether the system will send e-mails in HTML or Plain Text format. This is a global setting that applies to all e-mails; it is not user configurable.

**To specify HTML or Plain Text e-mail format**

1. Do one of the following:
   - In the IIS Manager, [Open the EFTAdHoc properties.](#)
   - Open `web.config` *(located by default in `C:\inetpub\EFTAdHoc\`) in a text editor.*

2. Edit the variable **EmailTemplateFormat**.
   - For HTML, set the variable to 0.
   - For Plain Text, set the variable 1.

3. After you have edited the configuration, do one of the following:
   - Click **OK** to close the dialog boxes, then, in the IIS Manager, click **File > Close**.
   - Save the `web.config` file.

It is not necessary to restart the service or reboot.

The system determines which set of e-mail templates to use, Plain Text or HTML, based on the value of **EmailTemplateFormat**.

Refer to [Secure Ad Hoc Transfer’s Configuration File](#) for details of variables used in the configuration file.
CREATING A COMMAND

The procedure below describes how to create a command that you can execute with an Event Rule.

**To create a command**

1. In EFT Administrator, connect to EFT Server and click the **Server** tab.
2. In the left pane, expand the Site node for the Site that you want to configure, then click **Commands**.
3. In the right pane, click **New**. The **Command** tab appears.

4. In the **Command Name** box, type the name of the command. You will reference the Command Name in the Event Rule pane and **Custom Command** dialog box (in the **Select Command** drop-down menu), so you should give the Command an intuitive name. For example, instead of **Command 1**, you might call it **Run CScript**.

5. Type a **Description** that will help you identify the command.

6. In the **Executable** box, browse to or type the path to the executable. For example, you can specify a program, a batch file, or a Windows scripting executable (e.g., `C:\Windows\system32\cscript.exe` or `wscript.exe`).

7. The **Redirect output to client** check box is used in the extremely rare case in which the command will be launched by a connecting FTP client (if configured to do so). If you select **Redirect output to client**, the result is sent to the connecting FTP client in a 220 message response. In the majority of cases, you should leave the check box cleared.

8. To create a log in the EFT Server installation folder, `cmdout.log`, that you can use to troubleshoot the command in case of failure, select the **Redirect output to system log** check box.

9. Leave all fields in the **Advanced** tab alone if you will be running a command from EFT Server’s Event Rule system (most common scenario) and skip to step 11. In the rare case this command will be launched from a connecting FTP client, type the parameters (if any) that will be passed to the command line. The variable format used is `%N%`. You may specify multiple variables or hard-coded values. (For example: `-c %1% %2%`).
10. If you want to force the FTP client to send a minimum number of parameters, select the Require parameters check box and specify the minimum number of parameters required. You can also write a message in the Invalid parameter count message text box that users will receive when the parameter number is not met.

11. If you want EFT Server to return an error if the launched process fails to respond, select the Enable process timeout check box and specify the number of seconds EFT Server should wait before terminating the command.

12. If you want a connecting FTP client to execute the command, click the Permissions tab and verify that the appropriate users have permissions to run the newly created command. If you only want to allow EFT Server to run the command (from the Event Rule system), leave the Permission tab as is.

13. Click Apply to save the changes on EFT Server.

### ENFORCING COMPLEX PASSWORDS FOR TEMPORARY USERS

When using EFT Server with the Secure Ad Hoc Transfer (SAT) module, if the password settings are set to use a minimum of more than 20 characters, the SAT temporary user creation will fail. If your Site's complex password settings require more than 20 characters, be sure to configure the EFTAdHoc Settings Template to override the Site's password settings so that complex passwords for SAT temporary users contain fewer than 20 characters.

### USING THE HS MODULE WITH THE SECURE AD HOC TRANSFER MODULE

Certain security features in the HS module (e.g., administrator password expiration and forced reset) are not compatible with the Secure Ad Hoc Transfer Module. If you are using the HS module and the SAT module with EFT Server, you should create a separate, non-PCI DSS Site that is used only for the Secure Ad Hoc Transfer module. You can disable the features that are not compatible, but that would take the Site out of compliance with the PCI DSS.
Administrator password expiration and forced reset are features that help your Site remain in compliance with the PCI DSS; however, those same features can cause problems with the SAT module. If the administrator password expires or changes, the value stored in the SAT module’s configuration file is no longer valid. Since the value stored in the configuration file is not plaintext, you cannot change it by typing the new password in the file. (Refer to Creating a Base64-Encoded Password for the procedure for encoding the password, which you can then paste into the configuration file.)

If your Site’s complex password settings require more than 20 characters, be sure to configure the EFTAdHoc User Settings Template to override the Site’s password settings so that complex passwords for SAT temporary users contain fewer than 20 characters.

The SAT module uses a temporary user account to upload files from the IIS computer to the temporary user’s home directory on EFT Server. If the UploadProtocol value in the configuration file is set to anything other than -1 (file copy), the file cannot be uploaded to the temporary user account, because the password has not been reset on first logon, as required for PCI DSS compliance. When UploadProtocol is set to anything other than -1 (the default is 5), the force reset password feature should be disabled.

The "force users to reset their password on initial login" option can be enabled on an HS-enabled Site, if the UploadProtocol setting in the configuration file is set to -1 (which means File Copy). Since this is not the default option, an EFT Server administrator must edit the file. Also, setting UploadProtocol to -1 (File Copy) is only a viable option if both EFT Server and IIS are installed on the same computer. The available settings for the UploadProtocol value are:

-1 = File copy  
0 = FTP  
1 = FTPS_IMPLIXCIT  
2 = FTPS_EXPLICIT  
3 = SFTP2  
4 = HTTP  
5 = HTTPS  
6 = SOCKS4  
7 = SOCKS5  
8 = FTPS_AUTH_TLS

The recommended configuration is to create a non-PCI Site for exclusive use by the SAT module, and disabling the password expiration and forced reset options. As always, if you have any questions or concerns regarding installing and configuring EFT Server for use with any of the modules, contact GlobalSCAPE Technical Support.
USING THE SECURE AD HOC TRANSFER MODULE

The topics below provide information regarding using the Secure Ad Hoc Transfer module.

SENDING FILES

You can transfer files of any type, but the file size is limited to 2GB or less. (This is a limitation of Web browsers, not the Secure Ad Hoc Transfer module.)

To send a file using Secure Ad Hoc Transfer

1. Connect to the Web e-mail interface. To do so, type the IP address or domain name to the IIS Web Site running the Secure Ad Hoc Transfer module, depending on the Web site and Virtual Folder you chose during installation. For example, type 192.168.20.156/EFTAdHoc or www.eftadhoc.com.

   The Web e-mail form appears:

   ![Web email form]

   If the Web form does not appear, try http instead of https. (Administrators can refer to Troubleshooting Errors in the Secure Ad Hoc Transfer Module for assistance.)

2. In the From box, type your e-mail address. The From address is stored in a cookie for one day after a successful e-mail has been sent. Subsequent e-mail messages contain the previous From e-mail address, unless you overwrite it.)

3. In the To box, type the destination address (the intended recipient), or click To to open your address book, which contains addresses you used previously. You can add multiple addresses separated by semicolons.

4. To show the Cc and Bcc boxes (advanced e-mail options), on the menu bar, click Show Cc & Bcc. Type the destination address (the intended recipient) or click Cc or Bcc to open your address book, which contains addresses you used previously.

5. To type multiple recipients, separate the addresses with commas; e.g., email1@bcd.com, email2@fsr.com.

6. If you want to send a copy of the message your e-mail address, on the menu bar, click Send me a copy.
7. If you want the recipient to be able to send you files, on the menu bar, click **Allow the recipient to send me a file**, which enables upload permissions to the temporary folder created for the recipient.

8. (Optional) In the **Subject** box, type the topic of the e-mail.

9. (Optional) In the **Body** box, type a message.

10. In the **Attachments** area, click **Add Files** to attach one or more files to the e-mail. A new file box and **Browse** button will appear (attachments are not required if **Allow Upload** is selected).

11. The **Add Files** button changes to **Add more files**. Repeat this process to attach more files.

12. To remove attachments, click **Remove** next to the attached file.

13. Click **Send**. A message appears indicating a successful send. When the transfer is complete, you will receive a confirmation message. The recipients will receive a message notifying them of the files to be picked up.

SMART E-MAIL FUNCTIONALITY

"Smart E-mail" functionality allows Secure Ad Hoc Transfer to pull e-mail addresses from EFT Server users' details. The **To**, **Cc**, and **Bcc** boxes can complete the e-mail address automatically if the address of the user (in any Settings Template other than the **EFTAdHoc** Settings Template) has both the user's name and e-mail address defined. Click **Show Cc & Bcc** if the **To**, **Cc**, and **Bcc** boxes are hidden.

---

*The **EFTAdHoc** Settings Template is a component of EFT Server.*
INCLUDING CC AND BCC RECIPIENTS

By default, the Cc and Bcc address boxes are hidden.

To display them, on the menu click Show Cc & Bcc.

To hide the boxes, click Show Cc & Bcc again.

You can use the Cc and Bcc boxes just as you do the To box. You can add multiple addresses separated by commas.

PERSONAL ADDRESS BOOK

When you type an address in the To, Cc, or Bcc boxes, a cookie is created. The box retains the address until you overwrite it so that you do not have to type it in every time you send an e-mail. The cookie expires every 24 hours.

To choose recipients from your address book

1. Click To, Cc, or Bcc. "My Address Book" appears containing any addresses previously used within the past 24 hours.
Secure Ad Hoc Transfer Module for EFT Server v6.1

2. Click the recipient to add. The address book closes and the address appears in the To, Cc, or Bcc box.

PICKING UP FILES

When a file is sent using Secure Ad Hoc Transfer, the recipient receives an e-mail message with a secure HTTP hyperlink, and a login username and/or password. (The Server administrator has the option of sending a hyperlink to allow One-Click Authentication.)

To pick up a file

1. In the e-mail, click the hyperlink.

2. If a login page appears, copy and paste the username and password from the e-mail to login dialog box, then click OK.

   • If using the Web Transfer Client:
     o To download a file, double-click the file in the Remote Server Files and Folders to transfer it to your local files and folders.
     o To upload a file, double-click the file in the local filesystem pane to transfer it to the remote filesystem.

   • If using the HTML Listing and Upload page, a list of files available for download appears.
     o To download a file, click a file name.
     o To upload a file, click Browse, click a file to upload, then click Upload.
ALLOWING RECIPIENTS TO UPLOAD FILES

As the sender (originator) of a file using Secure Ad Hoc Transfer, you can authorize the recipient to upload a file that you can later retrieve. For example, you can send a document to a reviewer, then the recipient can make edits to the document and upload the edited document. When the recipient uploads the file, you receive a notification e-mail that contains the same hyperlink and login credentials that were provided to the recipient.

When you send a file using Secure Ad Hoc Transfer, on the menu, click Allow Upload.

VIEWING REPORTS OF SAT ACTIVITY

With EFT Server's Auditing and Reporting module (ARM), you can generate reports of SAT activity. You do not have to configure anything extra in the SAT module--if the ARM module is installed, licensed, configured, and enabled, it is collecting SAT data that you can use in ARM reports. The predefined SAT reports provide the time the e-mail was sent, Site name, From e-mail address, To e-mail address, Subject line of the e-mail, e-mail type, attached file name, file size, expiration date, and temporary user name.

- **Activity-SAT by File (Detailed)** - This report displays all Secure Ad Hoc Transfer module activity for a specified file name, and sorted by date in reverse chronological order. If a user sent multiple files on one e-mail via the SAT module, each of the files are listed in the report.

- **Activity-SAT By Recipient (Detailed)** - This report displays all Secure Ad Hoc Transfer module activity for a specified recipient’s e-mail address, and sorted by date in reverse chronological order. If a user sent multiple files on one e-mail via the SAT module, each of the files are listed in the report. When you click Show Report, the Enter Report Parameters dialog box appears. Provide the entire e-mail address.

- **Activity-SAT by Sender (Detailed)** - This report displays all Secure Ad Hoc Transfer module activity for a specified sender’s e-mail address, and sorted by date in reverse chronological order. If a user sent multiple files on one e-mail via the SAT module, each of the files are listed in the report. When you click Show Report, the Enter Report Parameters dialog box appears. Provide the entire e-mail address.

- **Activity-SAT (Detailed)** - This report displays activity for Secure Ad Hoc Transfer module activity, sorted by date in reverse chronological order. If a user sent multiple files on one e-mail via the SAT module, each of the files are listed in the report.

- **Activity-SAT (Summary)** - This report displays all Secure Ad Hoc Transfer module activity, grouped by username, and sorted by date in reverse chronological order. If a user sent multiple files on one e-mail via the SAT module, each of the files are listed in the report.
TROUBLESHOOTING ERRORS IN THE SECURE AD HOC TRANSFER MODULE

Ideally, you will install IIS first, then .NET, then SAT. If you have already installed IIS, .NET, and SAT, you do not need to uninstall and reinstall everything, but you will have to re-register IIS using the ASP.NET registration tool after you install .NET. If you are using SAT on a 64-bit system, you will just need to allow 32-bit applications in IIS and run the ASP.NET registration tool (in that order). For other IIS7 and SAT errors, refer to the articles below and Knowledge Base article Q10510 - FIX: Secure Ad Hoc Transfer errors with Microsoft IIS 7.

FAILED TO CONNECT TO EFT SERVER

A variety of problems can cause SAT to be unable to connect to EFT Server, as described in this Troubleshooting chapter. A common problem is that incorrect values were chosen during installation (e.g., the wrong IP address or port number was provided) or IIS, .NET, and SAT were not installed in that order (in which case you will need to re-register IIS with .NET). If you receive the error below, verify the values supplied for configuration variables in the configuration file.

AD HOC PROPERTIES MISSING ASP.NET TAB

To edit the Secure Ad Hoc Transfer (SAT) Module configuration file, open the IIS Manager, expand the tree to find the SAT Module Web site, then right-click the node and click Properties. The Properties dialog box should have a tab called ASP.NET from which you can edit the configuration file.
Troubleshooting Errors in the Secure Ad Hoc Transfer Module

If that tab does not exist, either the .NET framework is not installed on the computer or .NET is not registered with IIS. The SAT Module installer should detect this and provide an error message. Before installing the SAT Module, ensure that IIS is set up with .NET.

- If you do NOT have the .NET framework installed on your system, you can download and install it from the Microsoft Developer Network.

- If you have the framework installed, but IIS still does not show any .NET-related information (such as the ASP.NET tab) or you cannot connect to \EFTAdhoc, run the ASP.NET IIS Registration Tool found in the .NET installation folder (e.g., C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727). The file is called aspnet_regiis.exe and you must pass in a "-i" parameter.

  The .NET 3.5 directory does not contain the registration tool executable; it is in the v2 directory. 3.5 is sort of a “service pack” to .NET 2.0. Even though you have .NET 3.5 installed, you must change directory to the one in the procedure below, because that is where the registration tool is located.

To run the ASP.NET Registration Tool

1. At command prompt, change to the directory that contains the executable. For example, type:

   cd WINDOWS\Microsoft.NET\Framework\v2.0.50727

2. Type the following, then press ENTER:

   aspnet_regiis.exe -i

   ASP.NET is installed and registered.

"CURRENT IDENTITY DOES NOT HAVE WRITE ACCESS"

The following error message can appear after installing Secure Ad Hoc Transfer:

"The current identity (NT AUTHORITY\NETWORK SERVICE) does not have write access to <framework directory>.
"

This error can occur on a Windows 2003 computer when Microsoft .NET 3.5 is installed BEFORE Microsoft IIS is installed. If this occurs, simply provide the network service with write access to the framework directory (e.g., C:\WINDOWS\Microsoft.NET\Framework\v3.5).

Refer to Ad Hoc Properties Missing ASP.NET Tab for the procedure for registering ASP.NET, which often fixes the problem.

FAILED TO ACCESS IIS METABASE

On operating systems before Windows 2008, this error can indicate that the .NET Framework is not registered with IIS. The .NET Framework detects which versions of IIS exist when the .NET Framework is installed, and it automatically registers itself with IIS. If IIS does not exist when .NET Framework is installed, the .NET Framework is not registered with IIS. Reinstalling IIS after the .NET Framework has been installed does not help.

If you receive this error, run the ASP.NET IIS Registration Tool, a program that comes packaged with the .NET Framework, to register it with IIS. Refer to AdHoc Properties Missing ASP.NET Tab for details.

Below is an example of an error caused by .NET Framework not being registered with IIS:
Troubleshooting Errors in the Secure Ad Hoc Transfer Module

PROBLEM Sending LARGE FILES

If you expect to upload large files, e.g., 1 GB or larger, we strongly recommend that you install EFT Server on the same computer as IIS and edit the value for UploadProtocol in the Secure Ad Hoc Transfer's Configuration File.

SAT MODULE APPLICATION ERROR CODES

When errors occur during the operation of the SAT module, an error number appears at the top of the SendMail form. Use the error code to troubleshoot the issue.

The table below provides descriptions for possible application errors that can occur with the SAT Module.

<table>
<thead>
<tr>
<th>Error</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10001</td>
<td>Not enough disk space to upload the files on drive {0} strTempFolderName</td>
</tr>
<tr>
<td>10003</td>
<td>The system could not save files to temporary directory</td>
</tr>
<tr>
<td>10006</td>
<td>The caller does not have the required permission to create the specified path (LogPath).</td>
</tr>
<tr>
<td>10007</td>
<td>The caller does not have the required permission to create the specified path (IISUploadFolder).</td>
</tr>
<tr>
<td>10008</td>
<td>The caller does not have the required permission to delete the uploaded File in the temporary directory.</td>
</tr>
<tr>
<td>10009</td>
<td>Unhandled Web exception. Refer to the log files for details.</td>
</tr>
<tr>
<td>10010</td>
<td>Unhandled exception. Refer to the log files for details.</td>
</tr>
<tr>
<td>10011</td>
<td>Failed to instantiate CIServer. Ensure SFTPCOMInterface.dll is registered on the application server.</td>
</tr>
<tr>
<td>10012</td>
<td>Could not initiate connection to EFT Server.</td>
</tr>
<tr>
<td>10013</td>
<td>The Site name {0} defined on the configuration file (web.config) cannot be found on EFT Server.</td>
</tr>
<tr>
<td>10014</td>
<td>The temporary user cannot be created on Site {siteName} of the EFT Server. Refer to the log files for details.</td>
</tr>
<tr>
<td>10015</td>
<td>Failed to set permissions for temporary user on Site {siteName} of EFT Server</td>
</tr>
</tbody>
</table>
### Error Description

<table>
<thead>
<tr>
<th>Error</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10016</td>
<td>Could not get a reference to the temporary user on Site {siteName} of EFT Server</td>
</tr>
<tr>
<td>10017</td>
<td>Could not set user home directory as root folder for Temporary user on Site {siteName} of EFT Server</td>
</tr>
<tr>
<td>10018</td>
<td>Failed to set expiration date for temporary user on Site {siteName} of EFT Server</td>
</tr>
<tr>
<td>10019</td>
<td>Failed to reset permissions for a temporary user on Site {siteName} of EFT Server</td>
</tr>
<tr>
<td>10020</td>
<td>Failed to send message by e-mail. Refer to log files for details.</td>
</tr>
<tr>
<td>10021</td>
<td>Expired Version</td>
</tr>
<tr>
<td>10022</td>
<td>Failed to instantiate ClientFTPEngineClass. Ensure ClientFTPCOMLib.dll is registered on the Application Server.</td>
</tr>
<tr>
<td>10023</td>
<td>Failed to get retrieved Settings Template for the EFTAdHoc Setting Template. Ensure the EFTAdHoc Settings Template was created on EFT Server. Refer to the log files for details.</td>
</tr>
<tr>
<td>10024</td>
<td>Complex password for the user could not be created on Site {siteName}</td>
</tr>
<tr>
<td>10025</td>
<td>Change password for the user could not be created on Site {siteName}</td>
</tr>
<tr>
<td>10026</td>
<td>Could not set New Full Name for the user.</td>
</tr>
<tr>
<td>10027</td>
<td>Access to the path is denied. Refer to the log files for details.</td>
</tr>
</tbody>
</table>

ℹ️ **maxRequestLength** = The maximum size allowed for a request, which is 4 MB by default. This includes uploaded files. Maximum request size can be specified in the Machine.config or Web.config file in the maxRequestLength attribute of the httpRuntime Element. Refer to Secure Ad Hoc Transfer's Configuration File for details of editing the file.