



# Secure Ad Hoc Transfer Module, v3

## *User Guide*

for  
EFT Server™  
v6.3 and later

**GlobalSCAPE, Inc. (GSB)**

---

**Address:** 4500 Lockhill-Selma Road, Suite 150  
San Antonio, TX (USA) 78249

**Sales:** (210) 308-8267

**Sales (Toll Free):** (800) 290-5054

**Technical Support:** (210) 366-3993

---

Web Support: <http://www.globalscape.com/support/>

© 2007-2012 GlobalSCAPE, Inc. All Rights Reserved

*Last Updated: April 23, 2012*

# Table of Contents

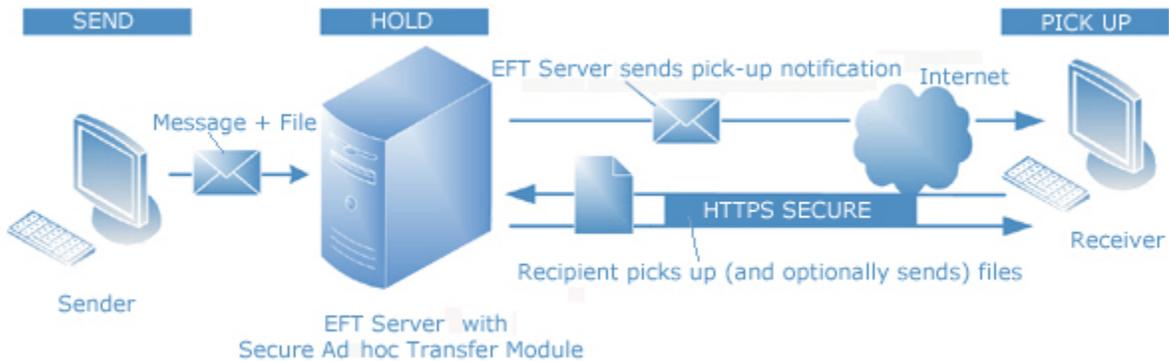
<b>Introduction to Secure Ad Hoc Transfer</b> .....	<b>5</b>
<b>What's New in the Secure Ad Hoc Transfer Module</b> .....	<b>5</b>
<b>Installing Secure Ad Hoc Transfer</b> .....	<b>7</b>
Secure Ad Hoc Transfer Module System Requirements and Installation Prerequisites .....	7
Secure Ad Hoc Transfer Deployment Methods .....	8
BEFORE Installing the SAT Module with IIS 7.0.....	9
Installing Secure Ad Hoc Transfer.....	10
Activating Secure Ad Hoc Transfer .....	17
Upgrading Secure Ad Hoc Transfer .....	18
Error message: "Unable to retrieve your e-mail address from the Active Directory server or e-mail address is invalid" .....	20
SAT Event Rules.....	21
AdHocRunCommand Custom Command .....	22
Uninstalling Secure Ad Hoc Transfer .....	23
<b>Configuring SAT</b> .....	<b>25</b>
The Secure Ad Hoc Transfer Module Administration .....	25
The SAT Administration Interface.....	26
Customizing the Secure Ad Hoc Transfer Web Interface.....	29
Background Color.....	30
Header Image Dimensions .....	30
Banner Background Style.....	30
Banner Image .....	31
Customizing the Notification E-Mail.....	31
Configuring Temporary-User Account Policy .....	32
Adding Blacklist and Whitelist Domains .....	33
Recipient Authentication Options .....	33
Specifying HTML or Plain Text E-Mail Format .....	34
Using SAT with Active Directory.....	34
Default Template Locations.....	35
Enforcing Complex Passwords for Temporary Users .....	35
Using the High Security Module (HSM) with the Secure Ad Hoc Transfer Module .....	35
Specifying Virtual Folders for SAT Users .....	37
<b>Using the SAT Module</b> .....	<b>39</b>
Sending Files .....	39
Picking Up Files.....	40

Viewing Reports of SAT Activity .....	41
<b>Troubleshooting Errors in the SAT Module .....</b>	<b>43</b>
Failed to Connect to EFT Server .....	43
Application Error: Unable to retrieve e-mail address from AD .....	43
SAT Module Application Error Codes .....	43
<b>Index .....</b>	<b>45</b>

## 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.

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 the SAT send mail page](#).
2. SAT 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), and a list of files available for download.
4. The recipient of the e-mail follows the HTTPS link (with embedded login credentials) and connects to the default HTTPS "plain text" interface or the Web Transfer Client.
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 using the recipient's login credentials. After seven days, the temporary account is removed from EFT Server's file system.
7. If Auditing and Reporting is enabled on EFT Server, all of the transactions associated with the Ad Hoc account are logged.

## What's New in the Secure Ad Hoc Transfer Module

In version 3 of the Secure Ad Hoc Transfer module, the [configuration](#) was moved from the web.config file to an XML-based configuration file, accessible from a web browser-based interface, provided for viewing and modifying the configuration. Various default values and the settings that are configured during the installation (e.g., EFT Server IP address) are populated in the web interface automatically.

Also added in version 3 are some [default Event Rules](#) in EFT Server to automatically send upload notifications, delete expired temporary users, and notify senders of upload(s) received from temporary users. The 2GB file limit was also removed.

For a complete version history, refer to the EFT Server release notes online at <http://www.globalscape.com/eft/history.aspx>.



# Installing Secure Ad Hoc Transfer

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

## Secure Ad Hoc Transfer Module System Requirements and Installation Prerequisites

The Secure Ad Hoc Transfer (SAT) module version 3 has been tested on Windows XP Professional, Windows Server 2003, Windows Server 2008 (Standard, Enterprise, and Datacenter editions) x86-64, and Windows 7 and requires the following:

- Connection to a computer running EFT Server v6.3 or later
  - If SAT is installed on a separate computer from EFT Server, EFT Server must be configured for remote administration.
- [Microsoft Internet Information Services \(IIS\)](#) Web Server version 6 or 7. (Ideally, you should install IIS first, then .NET, then EFT Server, then SAT.)
  - To use SAT with IIS7, you must [configure several options](#) BEFORE you install the software. On operating systems other than Windows 2008, you will need to install .NET Framework AFTER these features are enabled.
- [.NET Framework Runtime version 4 or later](#). (Install .NET before installing SAT.)
- An available connection to an SMTP mail server. Also refer to the following topics, if necessary:
  - [Allowing application servers to relay off Exchange Server 2007](#) (Microsoft Exchange Team Blog)
  - [How to troubleshoot mail relay issues in Exchange Server 2003 and in Exchange 2000 Server](#) (Microsoft KB article ID 895853)
- Java JRE 1.6 or later running on the client (sender/user) system that will be accessing the SAT Send Mail page. (In EFT Server v6.4.0, SAT's transfer engine was updated to use Java SE Runtime v6u26 and JFileUpload version 2.9C.)
- A web browser; SAT was tested on current (as of this release) versions Internet Explorer, Firefox, Safari (Windows and Mac OS), and Chrome browsers.

### **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 installer detects which version of IIS is installed.)
- 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 version 4 must be installed, configured, and running before installing the SAT module.
- Before installing the SAT module, you should have the following information available:
  - The EFT Server "server role" 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 and authentication credentials, if required
  - A SAT Module activation serial number (unless installing as a trial)

- The following settings should be configured in EFT Server before installing the SAT module:
  - Define a Site that uses GlobalSCAPE authentication or ODBC authentication. If SAT is using an AD or LDAP Site, it cannot create temporary users.
  - Enable Remote Administration in EFT Server.
  - Enable the HTTPS protocol in EFT Server at the Site level.
  - Temporarily disable password complexity for administrator accounts during the SAT installation. After SAT installation is complete, generate a new password for SAT, then update the password via the [SAT administration page](#). 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 SAT module. Or you can disable the features on the PCI DSS Site 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.

### 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**.

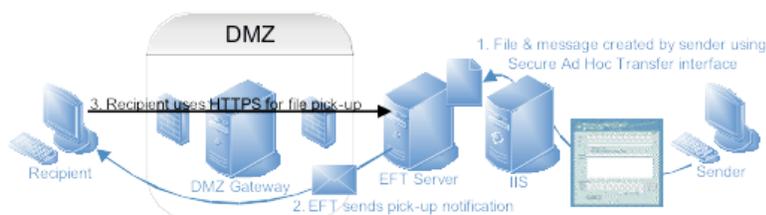
## Secure Ad Hoc Transfer Deployment Methods

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.

### Common Deployment Methods

- **Place IIS with SAT inside your network.** Access to the SAT interface is limited to internal users who can exchange files with external users.
- **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 as a mail relay.

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 page 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).

## BEFORE Installing the SAT Module with IIS 7.0

In order to install SAT correctly with IIS 7.0 you will need to enable (select) several IIS features. Most of the features that must be turned on for SAT are on by default; use the procedure below to verify these settings. (Refer to <http://technet.microsoft.com/en-us/library/cc753473.aspx> for more information about these features.)

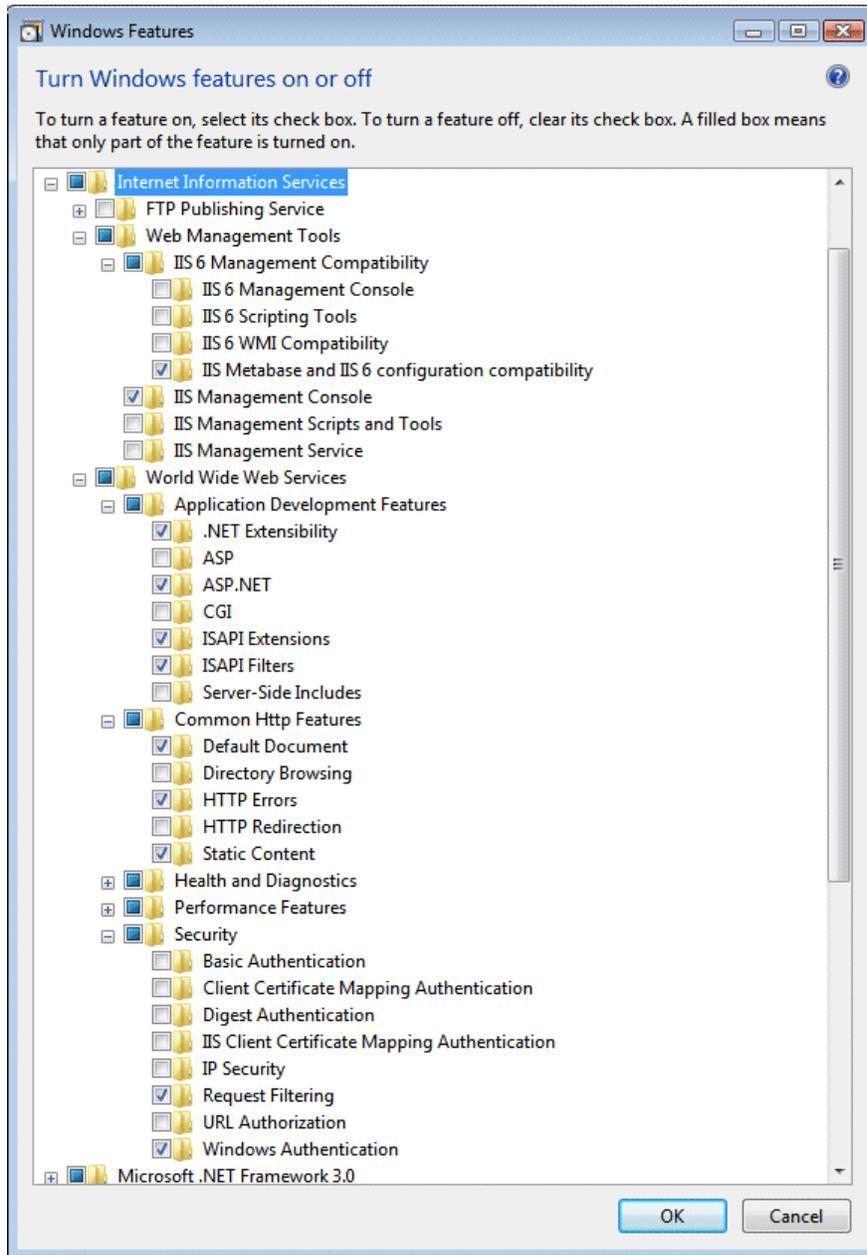
On operating systems other than Windows 2008, you will need to install .NET Framework AFTER these features are enabled. Refer also to article [#10510](#) in the GlobalSCAPE Knowledgebase.

- If EFT Server and IIS are NOT running on the same computer, copy EFT Server's **settings.config** file into the **SATScripts** folder after installing EFT Server and SAT.

### 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 6 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 below 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.**

- 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.
- If you are **not** installing SAT on the same computer as EFT Server:
  - Provide IIS a direct route and IP address to EFT Server.

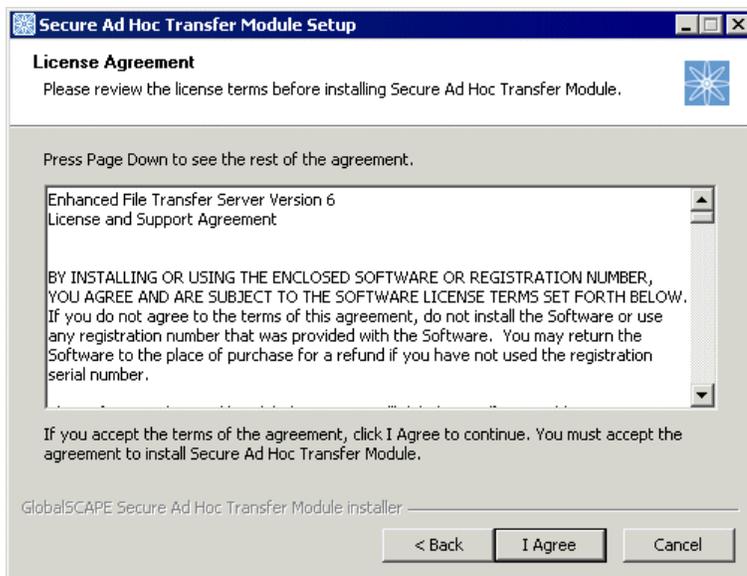
- Enable **Remote Administration** in EFT Server so that the installer can remotely configure EFT Server to use SAT.
- HTTPS must be enabled at the Site level so that the SAT scripts running on IIS can communicate with EFT Server.
- Also see [Next steps after installation](#) below the procedure for steps to follow after installation is complete.
- 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:
  1. Review the [system requirements, installation prerequisites, and decide on a deployment method](#).
  2. **On operating systems other than Windows 2008**, ensure IIS is installed BEFORE .NET is installed.
  3. 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

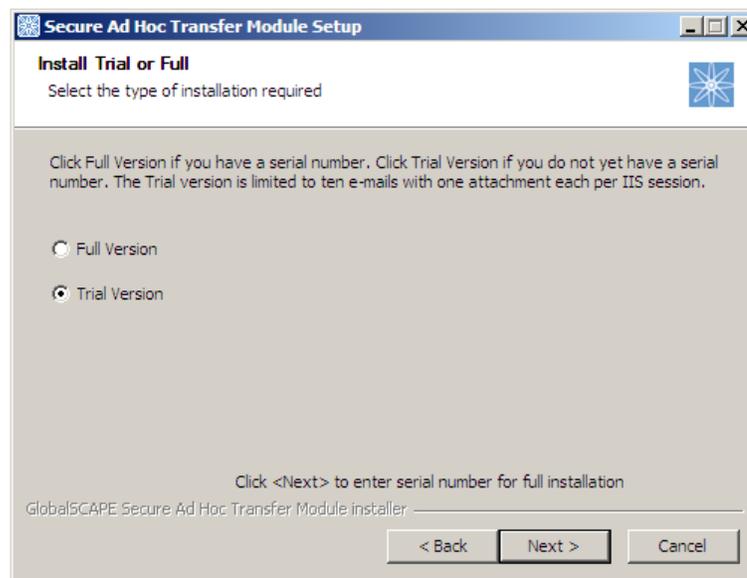
1. Copy the installer to the computer on which IIS and .NET are installed. (If they are not installed, install them before continuing. Refer to [Secure Ad Hoc Transfer System Requirements](#) for version details.)
2. Install EFT Server, create the Server object and at least one Site, and leave the EFT Server service running.
3. Double-click the installer. The installer wizard appears.
4. Click the drop-down menu, and then click **Secure Ad Hoc Transfer Module**.



5. Click **Next**. The **Welcome** page appears.
6. Click **Next**. The **Requirements Information** page appears.
7. Scroll through and read the requirements to ensure you have completed all requirements have gathered the necessary system information before continuing with the installation, then click **Next**. The **License Agreement** appears.



8. Read the license agreement and accept it by clicking **I Agree**. (If you do not accept the license agreement, the installer exits.) The **Install Trial or Full** page appears.



9. Do one of the following, then click **Next**:
  - If you are evaluating the SAT Module prior to purchase, click **Trial Version**. Any time during the Trial or after it expires, you can activate the SAT module.
  -

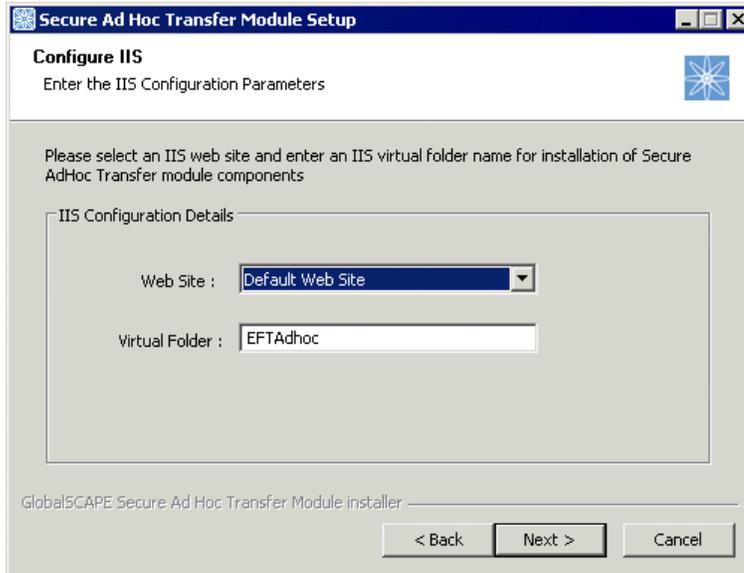
---

 *The trial version of SAT is not time limited; however, it is limited to ten e-mails with one attachment each, per IIS session.*

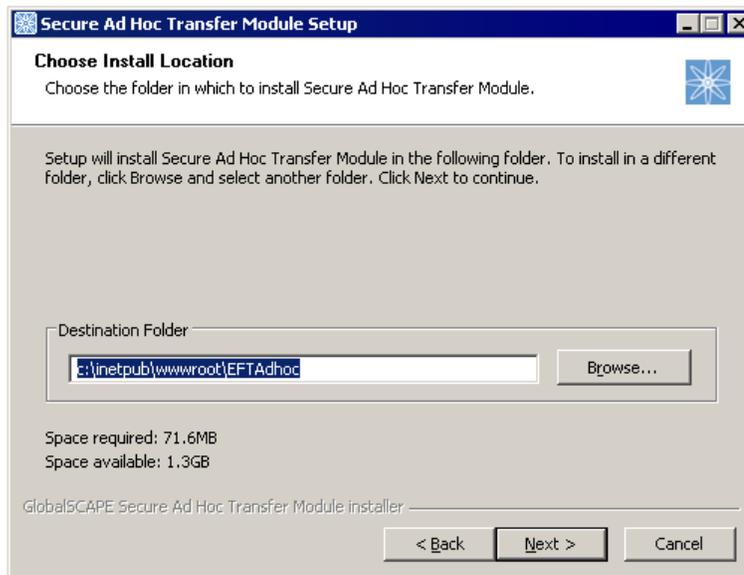
---

- If you have purchased the SAT Module, click **Full Version**. The **Serial number** page appears. Complete the activation information (to avoid errors, you can copy and paste the serial number from your invoice), then click **Next**.

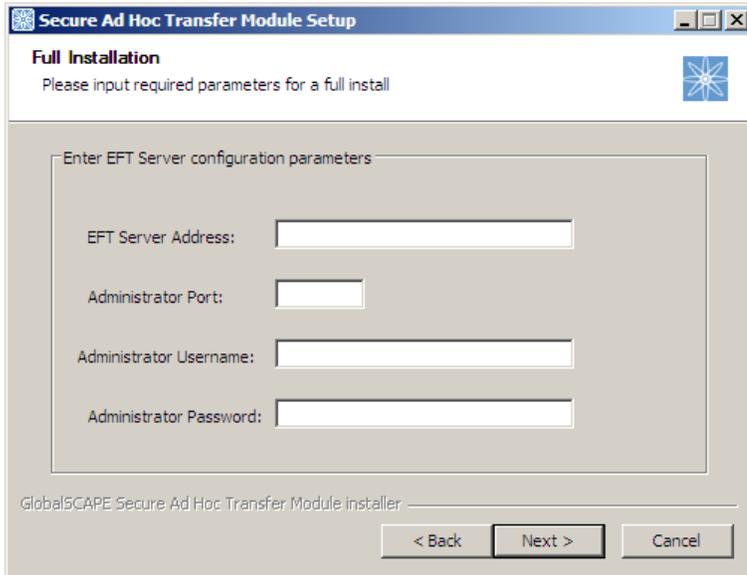
10. If a message appears stating that the installer did not detect the correct version of the Microsoft .NET Framework, click **Yes** to exit the installer and install the [correct version](#) of .NET Framework. If you know that the correct version is installed, you can click **No** to continue with the installation, then resolve the error later.
11. Click **Next**. The **Configure IIS** page appears.



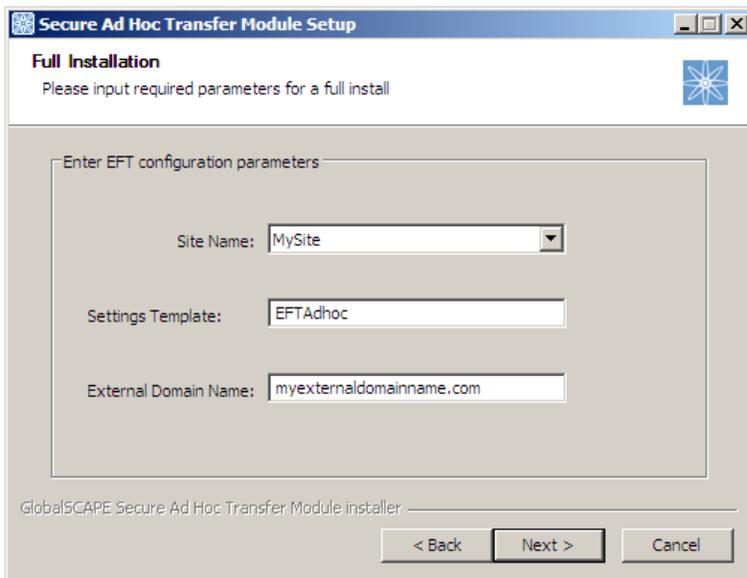
12. Specify a **website** and the **Virtual Folder** name (the default is **EFTAdHoc**) to use for the SAT components, then click **Next**. The **Choose Install Location** page appears.



- Specify the folder in which to install the SAT module (e.g., **C:\inetpub\wwwroot\EFTAdHoc**), then click **Next**. The **configuration parameters** page appears.



- Provide the EFT **Server name/IP** address, **Server Port** (1100 by default), and EFT Server **Administrator User Name** and **Password**, then click **Next**. The **Site Configuration Parameters** page appears.

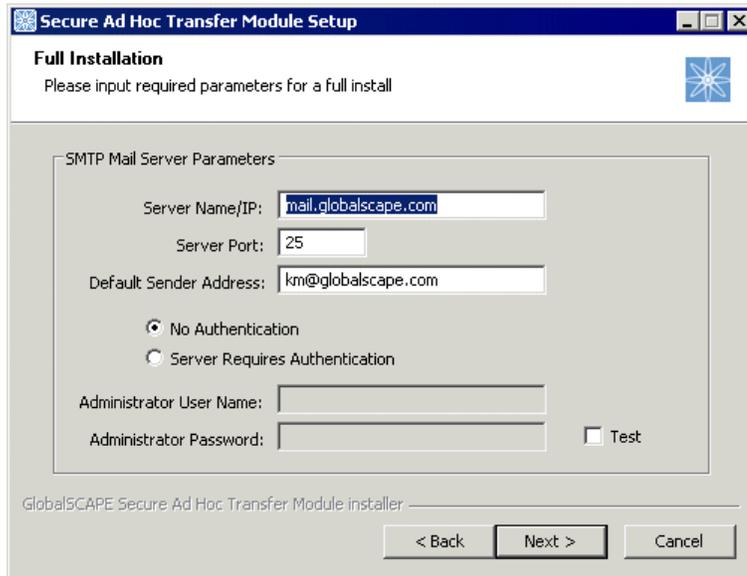


- If you have more than one Site defined in EFT Server, specify the EFT Server **Site Name** under which you want to install the SAT temporary users' Settings Template. Specify a Site that uses GlobalSCAPE authentication or ODBC authentication. If SAT is using an AD or LDAP Site, it cannot create temporary users.
- Provide a new, unique **Settings Template** name that will be used only for SAT (the default is **EFTAdHoc**).

17. Provide the **External Domain Name** for EFT Server. This is the external server address used to access EFT Server. Because e-mail recipients can be on an external network, you should use a DNS instead of the actual IP address. For example, type `myfileservers.com` (which might map to `https://10.0.0.100:444`).

 **IMPORTANT:** If you are also using DMZ Gateway, then use the address of DMZ Gateway instead.

18. Click **Next** to continue. The **SMTP Mail Server Parameters** page appears:



Secure Ad Hoc Transfer Module Setup

**Full Installation**

Please input required parameters for a full install

SMTP Mail Server Parameters

Server Name/IP:

Server Port:

Default Sender Address:

No Authentication

Server Requires Authentication

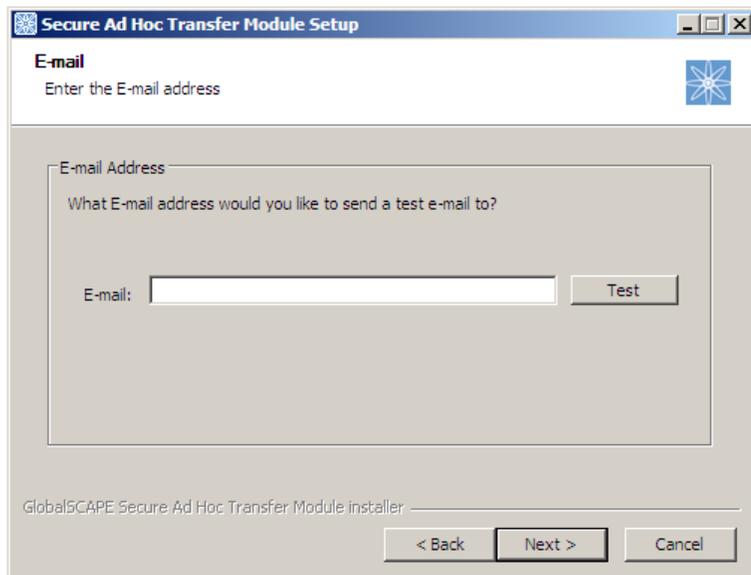
Administrator User Name:

Administrator Password:   Test

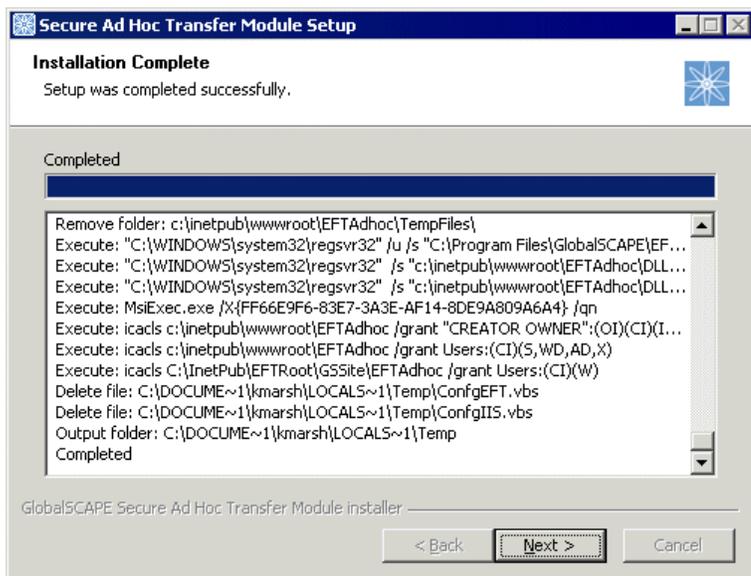
GlobalsCAPE Secure Ad Hoc Transfer Module installer

< Back   Next >   Cancel

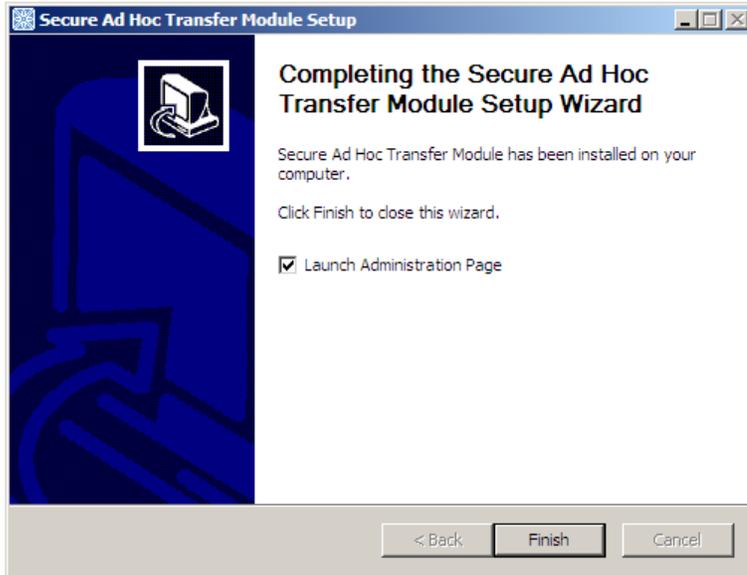
19. Even if you are installing the trial, provide the server parameters as if it were a Full installation. Type the SMTP **Server Name/IP** address, **Server Port**, and **Default Sender Address** (e-mail). If mail server authentication is required, click **Server Requires Authentication**, then type the **Administrator User Name** and **Administrator Password** used to connect to the mail server. If you want to test the SMTP mail server configuration settings, you can select the **Test** check box to send an e-mail to an accessible account.
20. Click **Next**. Provide the e-mail address for the test e-mail, click **Test**, then click **OK** after the "email has been sent" message appears.



21. Click **Next**. The SAT module is installed, and then a message appears telling you that the installer has created an EFT Server administrator account with minimal privileges for management of ad hoc accounts. This least-privileged account is necessary for IIS to communicate with EFT Server; IIS will not use your EFT Server "server role" admin account.
22. Click **OK** to dismiss the message. (Refer to the EFT Server help topic Adding Server Administrators for details of viewing or editing the account.)



23. A prompt appears telling you to refer to the help for additional configuration options. Click **OK**.
24. Click **Next**. The final screen appears.



25. If want to open the SAT administration interface, verify that the **Launch Administration Page** check box is selected, then click **Finish**.

---

#### Next Steps after installation:

---

A few additional steps may be necessary:

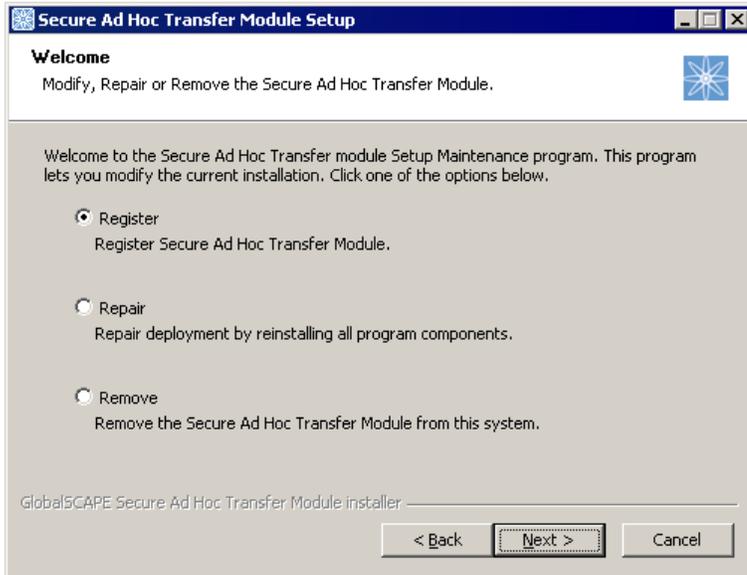
- The installer creates three [SAT-specific Event Rules](#) and a custom Command in EFT Server. The Event Rules and Command may need to be updated to reflect your system's paths.
- If EFT Server and IIS are NOT running on the same computer, copy EFT Server's **settings.config** file into the **SATScripts** folder after installing EFT Server and SAT.

### Activating Secure Ad Hoc Transfer

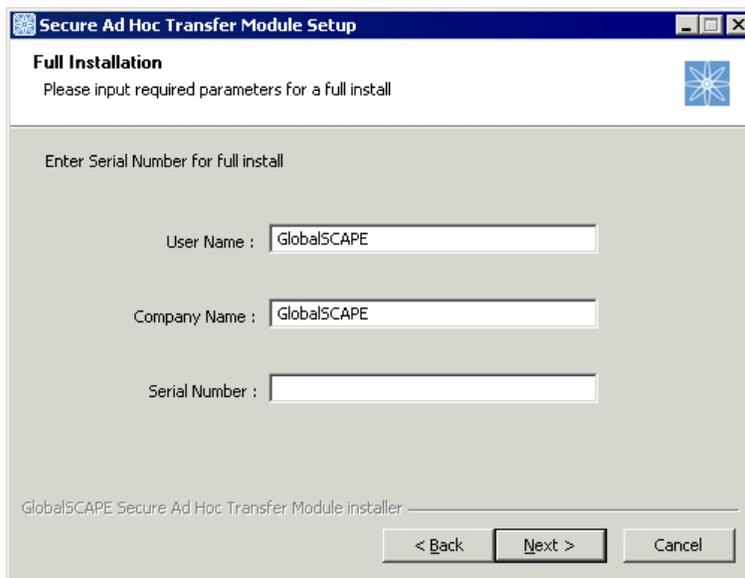
When you first install the Secure Ad Hoc Transfer module, you are given the choice of installing a Full or Trial version. The trial version is not time limited, but file sender operations are limited to ten per IIS session and a single file at a time. When you are ready to activate the SAT module, you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

#### To activate the full version

1. Execute the installer and accept the license agreement.



2. Click **Register**, then click **Next**.



3. 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

When you upgrade to a newer version of the Secure Ad Hoc Transfer (SAT) module, you should first upgrade EFT Server.

- 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.

---

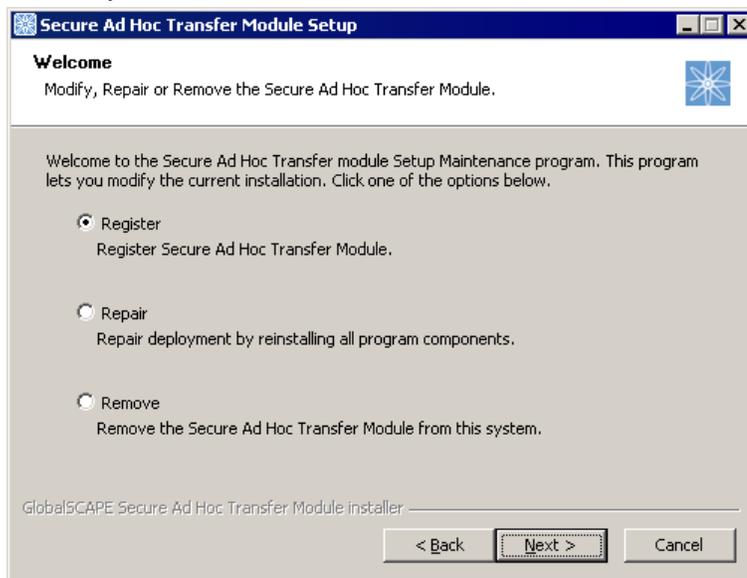
 *By default, **SFTPCOMInterface.dll** is stored in the EFT Server installation directory and in **C:\inetpub\EFTAdHoc** for the SAT module.*

---

- 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.
- If **Repair** is selected, the SAT installer merges the values located in the configuration file in the previous version with the corresponding variables in the new configuration file. The SAT installer creates a backup of all prior SAT files before installing the new files (in case of customizations).
- The SAT installer does NOT configure IWA when performing an upgrade.
- Upgraded SAT installations retain their prior anonymous authentication method. SAT version 3 allows Active Directory (AD) authentication for the sender by default (new installs). Optionally, you can turn off sender authentication (allow anonymous send) in the [SAT Administration pages](#). Refer to the **AD Extensions** section of the web interface for details of turning on or off sender authentication. After upgrading from version 2.x to version 3.x, if you enable sender authentication ("**Populate "From" e-mail address using Active Directory**"), end users will receive an error regarding retrieving e-mail addresses from Active Directory. Refer to [Error Message](#) below for instructions on how to address this issue.

### 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.



2. Click on of the following options, then click **Next**:
  - **Register**- Click **Register** if you have installed this version as a Trial and now want to upgrade to the Full version.
  - **Repair** - Click **Repair** if you are upgrading from a previous version.
3. Follow the prompts to complete installation.

### To restart IIS

1. Click **Start > Run**.
2. In the **Run** dialog box, type `iisreset`, then press ENTER.

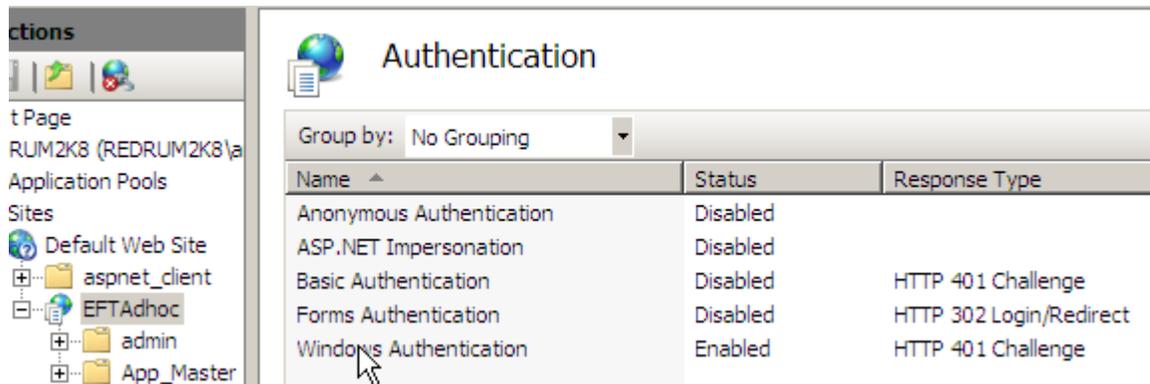
A command prompt appears, IIS is reset, and then the screen closes.

## Error message: "Unable to retrieve your e-mail address from the Active Directory server or e-mail address is invalid"

An error message stating that SAT is "Unable to retrieve your e-mail address from the Active Directory server or e-mail address is invalid" after upgrading from SAT version 2 to version 3, is caused by the fact that SAT retains the previous version's authentication settings when upgrading. If you want to use Integrated Windows Authentication (IWA), perform the procedure below.

### To use IWA with an upgraded SAT installation

1. Disable Anonymous Authentication and enable Windows Authentication in the following dialog box in the IIS manager:



2. In SAT's web.config file (by default, **C:\inetpub\wwwroot\EFTAdhoc\web.config**):
  - a. Change authentication mode to Windows:

```
<authentication mode="Windows" />
<roleManager enabled="false" />
<httpRuntime executionTimeout="600" maxR
<compilation debug="true" batch="false"
  <assemblies>
    <add assembly="System.D
```

- b. Add the following text to the <bindings> section of the file:

```
<bindings>
  <webHttpBinding>
    <binding name="SATBasicBin
      <readerQuotas maxD
    <security mode="TransportCredentialOnly">
      <transport clientCredentialType="Windows" />
    </security>
  </binding>
</webHttpBinding>
</bindings>
<services>
```

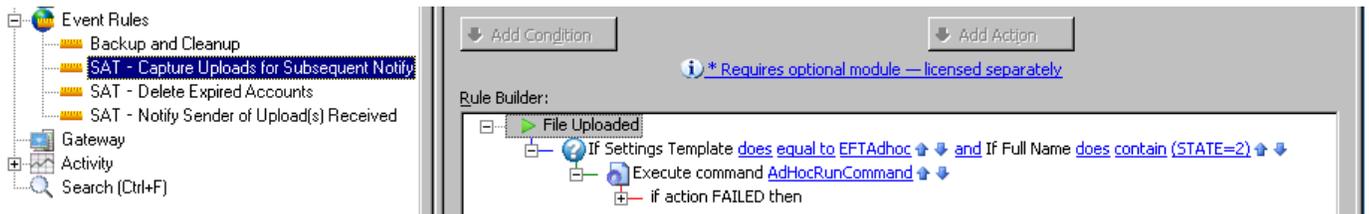
## SAT Event Rules

When you install version 3 of the Secure Ad Hoc Transfer (SAT) module, some "default" Event Rules are created by the installer.

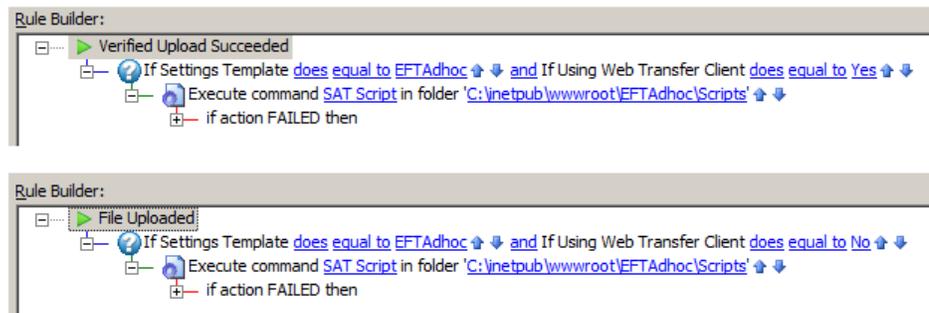
- If you are using a 64-bit system, the Event Rules and Command need to be updated to reflect the 64-bit paths. (Refer to the EFT Server documentation for details of Event Rules and Commands.)
- If EFT Server and IIS are NOT running on the same computer:
  - Copy the **setting.config** file from **C:\inetpub\wwwroot\EFTAdhoc\config\** to **C:\Program Files (x86)\GlobalSCAPE\EFT Server Enterprise\SATScripts\**.
  - Copy the templates from **C:\inetpub\wwwroot\EFTAdhoc\Templates\** to **C:\Program Files (x86)\GlobalSCAPE\EFT Server Enterprise\SATScripts\**.

See [below](#) for a description of the **AdHocRunCommand** Custom Command.

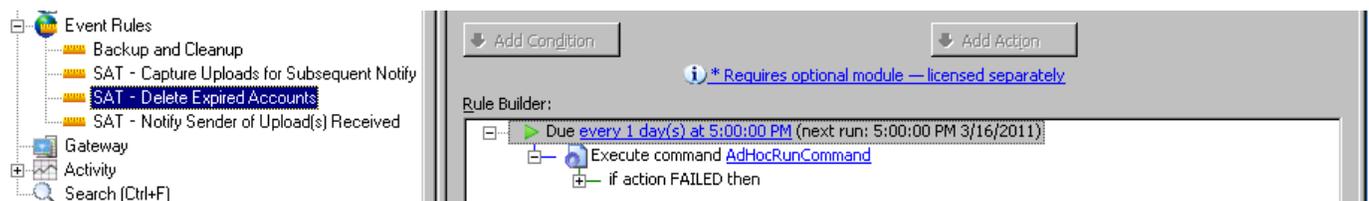
- **SAT - Capture Uploads for Subsequent Notify**—If the Settings Template is "EFTAdhoc" and if the remote IP address does not match \*.\*.\* (All Incoming), execute the **AdHocRunCommand** custom Command in **C:\Program Files\GlobalSCAPE\EFT Server Enterprise\SATScripts** to runs the **SendUploadNotification.wsf** script.



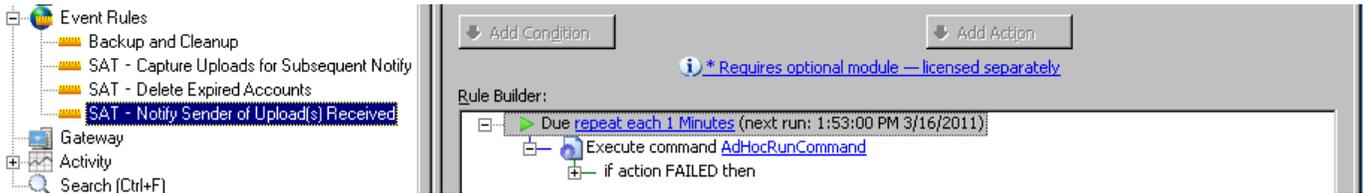
- i** The Rule above works best with the Plain-Text Client. If end users are uploading with the Web Transfer Client, add a second Rule using the "Verified Upload Succeeded" Event and add the Condition "If Using Web Transfer client does equal to Yes." Also add the "If Using Web Transfer client does equal to No" Condition to the Rule above.



- **SAT - Delete Expired Users**—Every day, execute the **AdHocRunCommand** custom Command in **C:\Program Files\GlobalSCAPE\EFT Server Enterprise\SATScripts** to run the **EFTDeleteExpiredUsers.wsf** script.



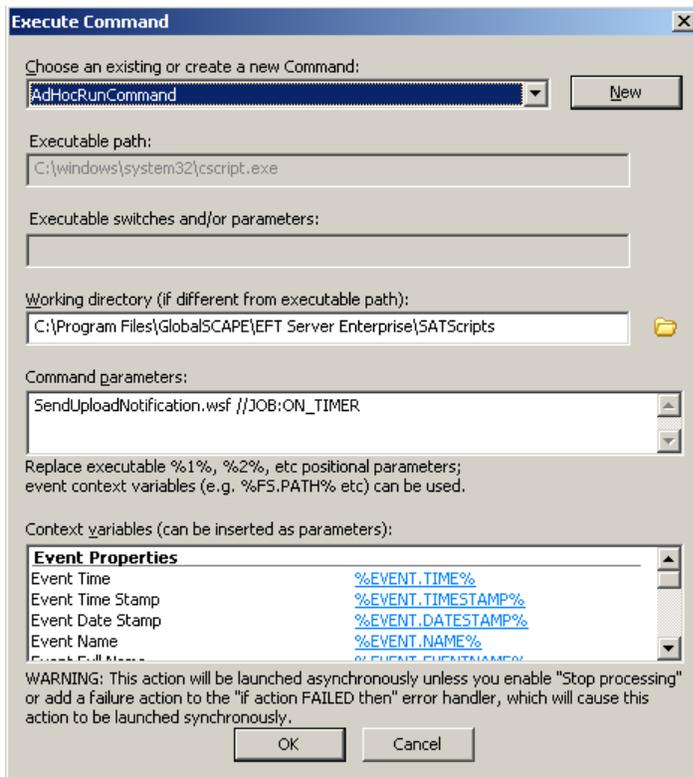
- **SAT - Notify Sender of Upload(s) Received**—Each minute, execute the **AdHocRunCommand** custom Command in **C:\Program Files\GlobalSCAPE\EFT Server Enterprise\SATScripts** to run the **SendUploadNotification.wsf** script.



These Event Rules automatically perform tasks that you had to configure manually in previous versions of SAT. The SAT Event Rules are enabled by default. You can edit the rules and disable them as needed. Refer to the "Event Rules" section of the EFT Server help for details of managing Event Rules.

### AdHocRunCommand Custom Command

The **AdHocRunCommand** Custom Command is created in EFT Server the when the SAT module is installed. **AdHocRunCommand** executes **C:\windows\system32\cmd.exe** (or **C:\windows\syswow64\cmd.exe** on 64-bit systems) and includes some custom **Command parameters** for executing the SAT scripts in the default SAT Event Rules.



- In the **SAT - Notify Sender of Upload(s) Received** Event Rule, **AdHocRunCommand** includes **SendUploadNotification.wsf //JOB:ON\_TIMER** in the **Command parameters** box.
- In the **SAT - Delete Expired Users** Event Rule, **AdHocRunCommand** includes **EFTDeleteExpiredUsers.wsf //JOB:DELETE\_USERS** in the **Command parameters** box.

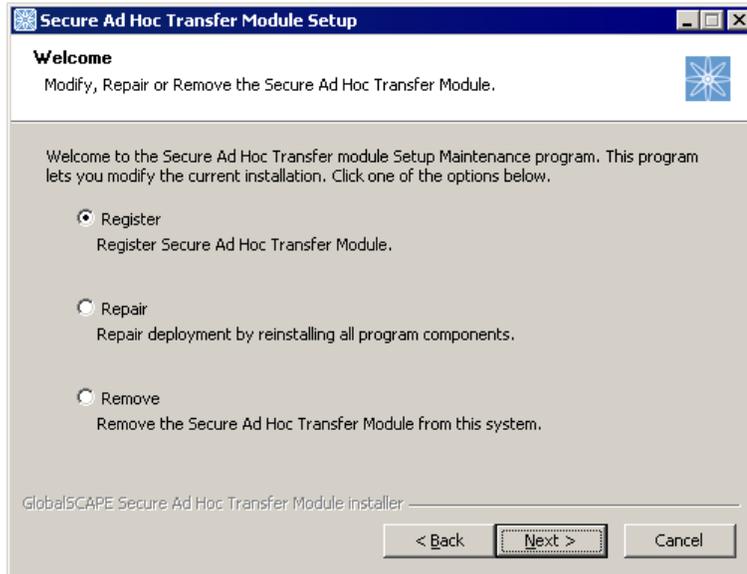
If you edit the custom Command, you might introduce errors, causing the script to not execute as designed. Instead, you should create a separate command, if necessary, and then you can add it as a subsequent Action to the Rule.

## Uninstalling Secure Ad Hoc Transfer

If you are upgrading from version 1.x of the SAT module, you must uninstall it before you can install the new version. You can use the Windows Programs and Features **Uninstall** tool or the procedure below.

### To uninstall Secure Ad Hoc Transfer

1. Run the installer for the new version. Refer to [Installing Secure Ad Hoc Transfer](#) for details, if necessary.



2. Click **Remove**, then click **Next**:
3. Follow the prompts to remove the software.



# Configuring SAT

After [installation](#) of the Secure Ad Hoc Transfer (SAT) module is complete, the help file and your default web browser appear. If your web browser does not display the SAT e-mail page, refer to [Troubleshooting Errors in the Secure Ad Hoc Transfer Module](#).

A few configuration options you may want to consider:

## A few configuration options you may want to consider:

- [The Secure Ad Hoc Transfer Module Administration](#)—Configuration is set during installation, but you can edit settings in the admin interface.
- [Customizing the Secure Ad Hoc Transfer Web Interface](#)
- [Customizing the Notification E-Mail](#)
- [Configuring Temporary-User Account Policy](#)
- [Adding Blacklist and Whitelist Destination Domains](#)
- [Recipient Authentication Options](#)
- [Specifying HTML or Plain Text E-Mail Format](#)
- [Using SAT with Active Directory](#)
- [Default Template Locations](#)
- [Enforcing Strong \(Complex\) Passwords](#)
- [Using SAT with the HSM](#)
- [Specifying Virtual Folders for SAT Users](#)

For advanced configuration options, please refer to the [GlobalSCAPE Knowledgebase](#). [GlobalSCAPE Professional Services](#) provides custom integration and branding services.

## The Secure Ad Hoc Transfer Module Administration

Hosted alongside the Secure Ad Hoc Transfer (SAT) module, a series of web pages is provided in which you can view and modify settings stored in the configuration file. The settings in the interface are populated with the values you provided when you installed the SAT module. It is not necessary to edit the configuration to start using SAT to send e-mails.

Starting in SAT v3.1, you can also access the Send Mail Page from within the administration interface.

You can access the administration interface by doing one of the following:

- Enter its address in your web browser (e.g., <http://localhost/EFTAdhoc/admin/>).
- Open it from the Start menu (**Start > Programs > GlobalSCAPE > Secure Ad Hoc Transfer Module > Secure Ad Hoc Administration**).
- Click the Secure Ad Hoc Send Page icon on the desktop.

---

 *If you are unable to connect to the Secure Ad Hoc Administration pages, ensure that the settings in the configuration file in the SAT installation folder are correct (by default, **C:\vnetpub\wwwroot\EFTAdhoc\config\settings.config**).*

---

### Considerations for SAT administration:

- In Windows 2003, make sure the administrator user has membership in the "Administrators" group.

- o In Windows 2008, each administrator user needs to be added individually to the administration folder. For example, using an administrator-elevated command window, the following command line should grant the currently logged in user permission to the directory:

```
icacls admin /T /C /grant %USERDOMAIN%\%USERNAME%:(OI)(CI)(F)
```

- o In Windows 2008, the user that installs SAT will automatically be added to the list of users allowed to access the administration interface.
- o It is a Windows standard to NOT allow logins for user accounts that do not have a password. Even if you have access to the folder, you will be denied access to SAT if you are attempting to login in with an account that does not have a password.

## The SAT Administration Interface

The SAT administration interface contains four pages with standard text boxes, check boxes, radio buttons, and drop-down list boxes. Each editable field has context-sensitive help provided in the interface. Be sure to click **Save** before navigating away from a page in which you changed settings.

- **General Settings**—On the **General Settings** page, you can set or change EFT Server connection settings, SMTP server connection settings, and SAT log (auditing) settings.

**Navigation**

- >> **General**
- >> **Advanced**
- >> **Security Policy**
- >> **AD Extensions**
- Send Mail Page**

**General Settings**

**EFT Server Connection Settings**

EFT Server administrator address:

EFT Server administrator port:

EFT Server administrator account name:

Ad hoc administrator account password:

EFT Server Ad Hoc Site:

EFT Server Ad Hoc Settings Template:

**SMTP Server Connection Settings**

Notification e-mail from address:

Send errors to admin e-mail address:

SMTP server address:  Port:

Authentication mode:

SMTP account name (optional):

SMTP account password (optional):

**SAT Log(Auditing) Settings**

Log Folder:

Log level:

- **Advanced Settings**—On the **Advanced Settings** page, you can set or change EFT Server address:port at which the SAT client application will upload files for retrieval by recipients, SAT host address for picking up files, and specify the format in which the e-mails are sent.

The screenshot shows the 'Advanced Settings' page. On the left is a 'Navigation' sidebar with links for 'General', 'Advanced', 'Security Policy', 'AD Extensions', and 'Send Mail Page'. The main content area is titled 'Advanced Settings' and contains the following sections:

- EFT Server Connection Settings**: A text input field for 'EFT Server file transfer address:port'.
- Ad Hoc Message Compose and Send**: A 'Wait' spinner set to '30' seconds before notifying sender after recipient uploads a file.
- SAT host address for picking up files:** A text input field.
- E-mail format**: Radio buttons for 'Send e-mails in HTML format' (selected) and 'Send e-mails in text format'. A checked checkbox for 'Include GlobalSCAPE's logo in e-mail'.
- A 'Save' button at the bottom.

- **Security Policy Settings**—On the **Security Policy Settings** page, you can set or change recipient password provisioning, specify domains to which you allow or deny e-mails to be sent, specify recipient folder upload-download permissions, and temporary account expiration and name length.

The screenshot shows the 'Security Policy' page. On the left is a 'Navigation' sidebar with links for 'General', 'Advanced', 'Security Policy', 'AD Extensions', and 'Send Mail Page'. The main content area is titled 'Security Policy' and contains the following sections:

- Access Control Policy**: A dropdown menu for 'Recipient password provisioning' set to 'Single-click authentication (user+pass embedded in link)'. A 'Delay' spinner set to '0' seconds before sending second e-mail containing the password.
- Radio buttons for 'Allow send to all domains except:' and 'Deny to all domains except:' with an associated text input field.
- Resources Control Policy**: Two columns of permissions for 'Recipient folder permissions (download only)' and 'Recipient folder permissions (download-upload)'. Each column has checkboxes for Upload, Download, Delete, Rename, Append, Show files and folders, Show read only files, Show hidden files, Delete folder, and Create folder.
- Temporary Account Policy**: 'Remove temporary account after' spinner set to '7' (days) and 'Temporary account name length' spinner set to '10' (characters).
- A 'Save' button at the bottom.

- **AD Extensions**—On the **AD Extensions** page, you can set or change whether SAT will try to obtain the currently logged on user's e-mail address from Active Directory to populate the **From** field, specify whether the **From** field is editable, and specify AD query attributes, search filter, and scope.

The screenshot shows the 'AD Extensions' configuration page. On the left is a 'Navigation' sidebar with links for 'General', 'Advanced', 'Security Policy', 'AD Extensions', and 'Send Mail Page'. The main content area is titled 'AD Extensions' and contains the following sections:

- Active Directory Extensions:** Two checkboxes: 'Populate "From" email address using Active Directory' (unchecked) and 'Disable "From" field (don't allow override) when using AD for populating e-mail address' (checked).
- AD Query Parameters:** A section header.
- Attributes:** A text input field containing 'cn,sAMAccountName,userPrincipalName,mail,displayName,sn'.
- Search Filter:** A text input field containing '(&(objectClass=person))((sAMAccountName=%USER.LOGIN%)(userPrincipalName=%USER.LO'.
- Attribute that identifies field as an e-mail:** A text input field containing 'mail'.
- Scope:** A dropdown menu set to 'Subtree'.
- Save:** A button at the bottom.

- In SAT v3.1 and later, you can click the Send Mail Page link to open the send mail page and verify your settings.

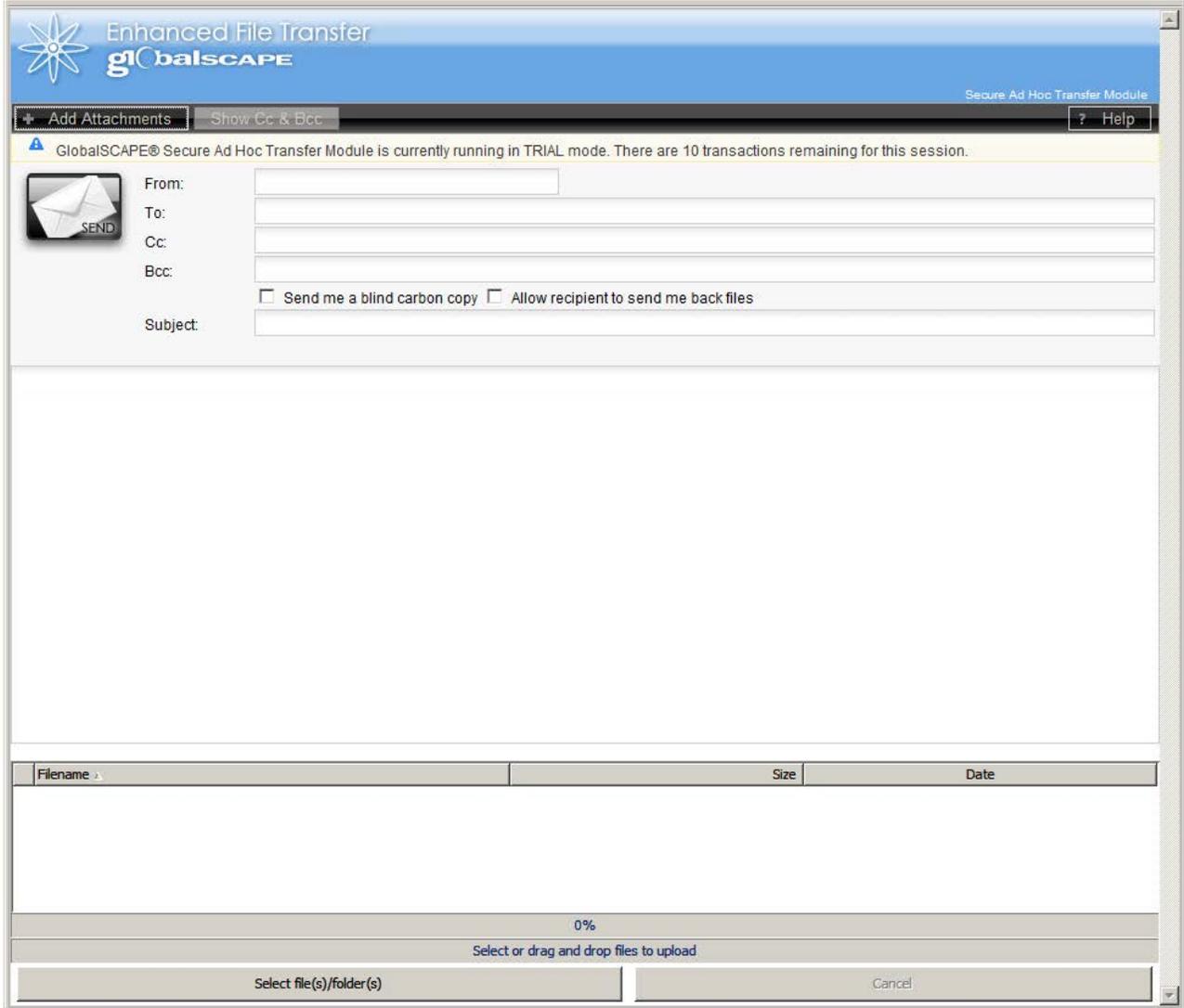
The screenshot shows the 'Send Mail Page' interface. At the top, there are buttons for 'Add Attachments' and 'Show Cc & Bcc', and a 'Help' button. A yellow warning banner states: 'GlobalSCAPE® Secure Ad Hoc Transfer Module is currently running in TRIAL mode. There are 10 transactions remaining for this session.' Below the banner is a 'SEND' button with an envelope icon. The form includes fields for 'From:', 'To:', and 'Subject:'. There are also two checkboxes: 'Send me a blind carbon copy' and 'Allow recipient to send me back files'.

## Customizing the Secure Ad Hoc Transfer Web Interface

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

 GlobalSCAPE's [Professional Services](#) can customize the interface based on your requirements.

The picture below shows the default appearance, with **Add Attachments** and **Show Cc & Bcc** buttons selected.



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

---

## Background Color

---

The default color behind the SendMail page 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 */
```

---

## Header Image Dimensions

---

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:

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

To

```
.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

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

To

```
.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:

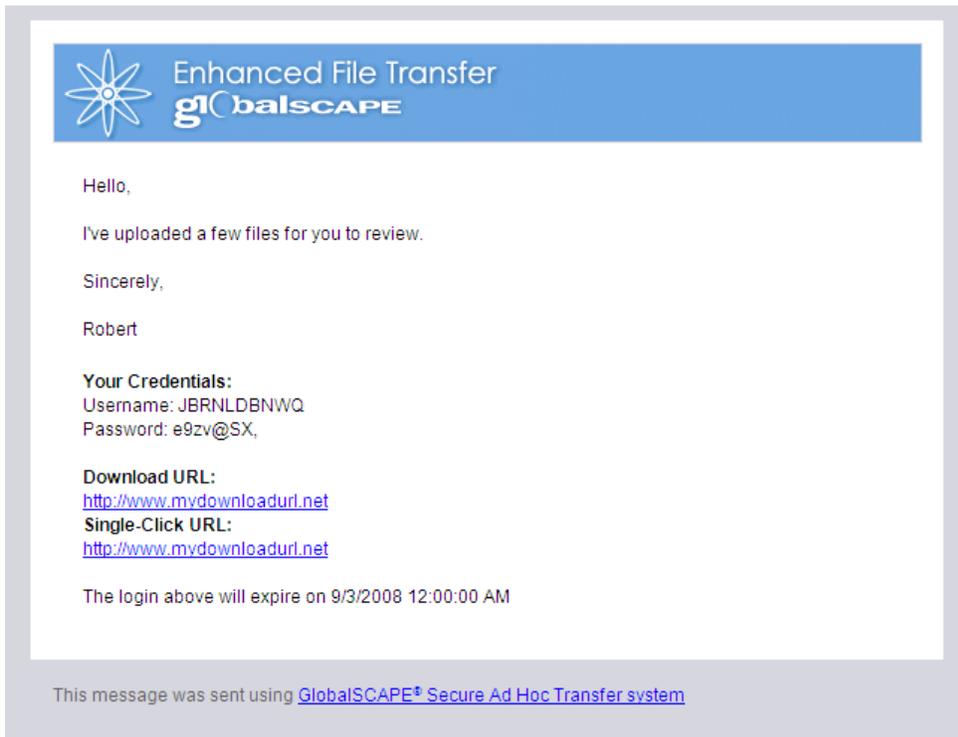
```
<asp:Image SkinID="Header_Logo" runat="server"
ImageUrl="~/App_Themes/DarkGray/images/banner-
adhoc.png" CssClass="Header_LogoStyle" />
```

To

```
<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 logo used for notification e-mails. That is, you can remove the logo from the e-mail or replace it with your own. GlobalSCAPE's [Professional Services](#) can provide other customizations based on your requirements. On the **Advanced** page of the [SAT administration interface](#), you can set or change Ad Hoc message composition and send options.



### To remove the GlobalSCAPE logo from e-mails

- On the **Advanced Settings** page of the SAT administration interface, clear the **Include GlobalSCAPE's logo in e-mail** check box, then click **Save**.

### To change this logo image

1. Copy the new logo image into the `\EFTAdhoc\Templates` folder (e.g., `C:\inetpub\wwwroot\leftadhoc\templates`).
2. In SAT's `/config/` directory, open the `settings.config` file in a text editor (e.g., `C:\inetpub\wwwroot\EFTAdhoc\config\settings.config`), modify the variable `ImageLogoFileName` with the new file name.  
For example, change:

```
<add key="ImageLogoFileName" value="email_logo.gif" />
```

To

```
<add key="ImageLogoFileName" value="your-image-here.jpg" />
```

## Configuring Temporary-User Account Policy

Temporary-user accounts are created when you send a file to a recipient that is not defined in EFT Server. On the **Security Policy** page of the SAT administration interface, you can configure the temporary-user account policy.

### To change temporary-user account policy

1. Log in to the SAT administration interface (e.g., **Start > Programs > GlobalSCAPE > Secure Ad Hoc Transfer Module > Secure Ad Hoc Configuration**).
2. In the left navigation page, click **Security Policy**. The **Security Policy** page appears.
3. Edit the settings as needed:
  - **Configuring temporary-user account expiration**—By default, 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 change the expiration period, change **Remove temporary account after: [ N ] (days)** to the number of days after which you want the account to expire or 0 (zero) if you do not want the account to expire.
  - **Configuring temporary user account name length**—By default, the name length is 10 characters. To change the account name length, change **Temporary account name length [N] characters** to the number of characters you want.
  - **Configuring temporary-user account permission**—EFT Server administrators can control which permissions are set when a SAT user toggles **Allow Upload** when sending an e-mail by editing the permissions in the **Resources Control Policy** area.
4. Click **Save** to save your changes on the Server.

## Adding Blacklist and Whitelist Domains

You can configure Secure Ad Hoc Transfer to block (Blacklist) or allow (Whitelist) only specific domains. That is, if you do not want users to send files to or from certain e-mail accounts, you would add that domain to the blacklist. The value applies to e-mail address in the **From**, **To**, **CC**, and **BCC** fields.

To block or allow specific domains

1. Log in to the SAT administration interface (e.g., **Start > Programs > GlobalSCAPE > Secure Ad Hoc Transfer Module > Secure Ad Hoc Configuration**).
2. In the left navigation page, click **Security Policy**. The **Security Policy** page appears.

- To allow e-mails to be sent to all domains EXCEPT one or more specified, click **Allow send to all domains except**, then specify the domains to which you want to prevent e-mails from being sent.
- To block e-mails from being sent all domains EXCEPT one or more specified, click **Deny to all domains except**, then specify the domains to which you want to ALLOW e-mails to be sent.

Separate multiple domains by commas.

3. Click **Save** to save the changes on the Server.

## Recipient Authentication Options

By default, SAT notification e-mails include a hyperlink to log the recipient in to the Web Transfer Client automatically to download the files that were sent. Optionally, you can configure SAT to provide login credentials in one email, separate e-mails (one with the username, another with the password), or just the username, with the password to be sent by other means, such as a phone call. You can also specify whether SAT users are allowed to send to only specified domains or are denied sending to specified domains.

### To change temporary-user Access Control Policy

1. Log in to the SAT administration interface (e.g., **Start > Programs > GlobalSCAPE > Secure Ad Hoc Transfer Module > Secure Ad Hoc Administration**).
2. In the left navigation page, click **Security Policy**. The **Security Policy** page appears.
3. In the **Access Control Policy** area, edit the settings as needed:

- **Recipient password provisioning**—Click the drop-down list to specify how the login credentials for retrieving files are provided to the recipient:
  - Username and password in same e-mail message
  - Username and password in separate messages
  - Username and password in separate messages (to sender, and then sender provides to the recipient by other means)

- Username (to recipient) and password (to sender, and then sender provides to the recipient by other means)
- Single-click authentication is specified (username and password are embedded in a link)
- **Delay [N] seconds before sending second e-mail containing the password**—When the username and password are sent in separate messages, you can specify a delay between sending each e-mail.

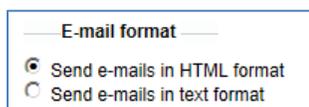
4. Click **Save** to save your changes on the Server.

## 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 whether e-mails are sent as plain text or HTML

1. Log in to the SAT administration interface (e.g., **Start > Programs > GlobalSCAPE > Secure Ad Hoc Transfer Module > Secure Ad Hoc Administration**).
2. In the left navigation page, click **Advanced**. The **Advanced Settings** page appears.
3. In the **E-mail format** area, specify a format, either HTML or text.



4. Click **Save** to save your changes on the Server.

## Using SAT with Active Directory

SAT allows Active Directory (AD) authentication for the sender by default (new installs). This page is for enabling AD extensions for restricting access to the SAT page; it has nothing to do with how the SAT module works in conjunction with EFT Server.



*If you plan to override SAT's Integrated Windows Authentication by modifying the configuration settings file's Path, DomainAdminUser, DomainAdminPass (base64 encoded), and AuthenticationMethod fields, you must also set "ConnectionSettingEnabled" value="True", otherwise those values will NOT be used by SAT.*

---

### To change Active Directory information in SAT

1. Log in to the SAT administration interface (e.g., **Start > Programs > GlobalSCAPE > Secure Ad Hoc Transfer Module > Secure Ad Hoc Administration**).
2. In the left navigation page, click **AD Extensions**. The **AD Extensions** page appears.
3. Edit the settings as needed:
  - **Populate "From" email address using Active Directory**—When the **Populate "From" email address using Active Directory** check box is selected, SAT will query the AD server for the email address of the currently logged in user to populate the **From** field on the **Send Mail** page. If this check box is selected when AD is **not** being used, SAT will get an application error.
  - **Disable "From" field (don't allow override) when using AD for populating e-mail address**—Select this check box when **Populate "From" email address using Active Directory** is selected if you do not want senders to change the "From" address.
  - **AD Query Parameters**—Edit these fields to match the AD server's parameters for finding e-mail addresses to populate the "From" address.
4. Click **Save** to save your changes on the Server.

## Default Template Locations

E-mail notifications are formatted by templates stored on the computer on which SAT is installed. (By default, stored in **C:\inetpub\wwwroot\EFTAdhoc\Templates.**)

- **ErrorReportMessage.tlt** and **ErrorReportMessage.txt**—When a SAT send event fails to work for any reason, a message box appears that allows the sender to send a notification to the SAT administrator. These templates provide the text of the e-mail notification.
- **PasswordMessage.tlt** and **PasswordMessage.txt**—One of two notifications sent to a temporary user when the login username and password are sent in separate emails. Includes the password, download URL, and an expiration date.
- **UsernameMessage.tlt** and **UsernameMessage.txt**—One of two notifications sent to a temporary user when the login username and password are sent in separate emails. Includes the username, download URL, and an expiration date.
- **UsernamePasswordMessage.tlt** and **UsernamePasswordMessage.txt**—Notification sent to temporary user when both username and password are sent in the same e-mail; contains login credentials, download URL, and expiration date.
- **SingleClickAuthenticationMessage.tlt** and **SingleClickAuthenticationMessage.txt**—Message sent when to temporary user when Single-Click Authentication (login credentials embedded in the link) is used; includes login credentials, a file list, a download URL, the single-click URL, and the date that the file download will expire.
- **SendUploadNotificationMessage.tlt** and **SendUploadNotificationMessage.txt**—When a SAT user sends attachments to a temporary user, and that temporary user is allowed to upload files in return, a notification that files were uploaded by the temporary user is sent to the SAT user. The notification includes the filename and location, the account credentials, the download URL, and the server time.

## Enforcing Complex Passwords for Temporary Users

If your EFT Server password settings are set to use a minimum of more than 20 characters, the SAT temporary user creation will fail. If your EFT Server 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.

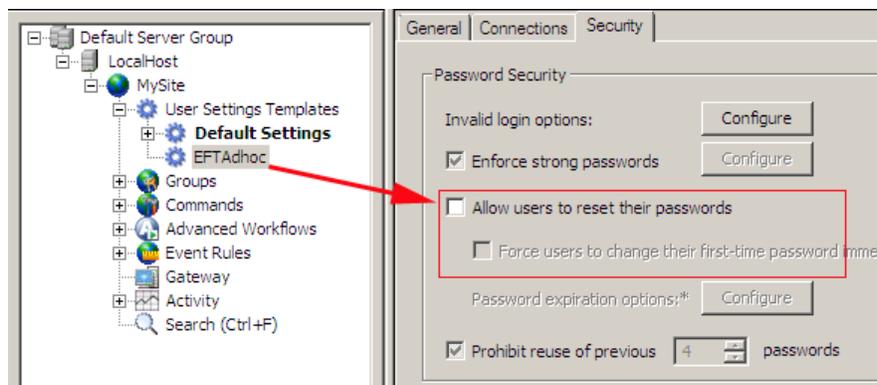
Refer to "Enforcing Complex Passwords at the Site Level" in the EFT Server documentation for more information about configuring complex passwords.

## Using the High Security Module (HSM) with the Secure Ad Hoc Transfer Module

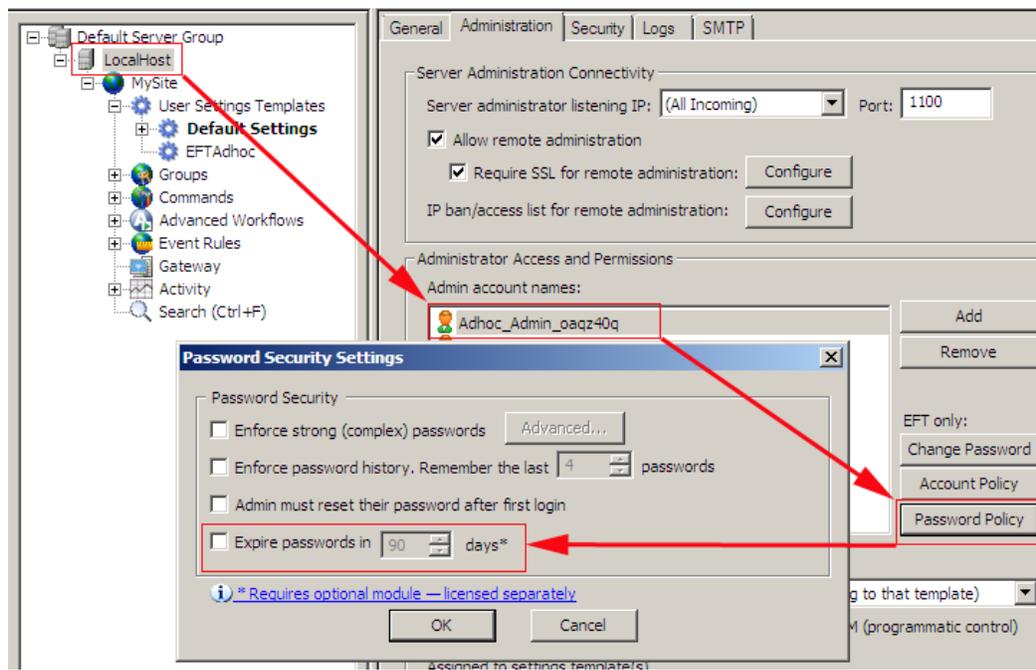
When installed with the default settings, SAT violates a couple of the Payment Card Industry Data Security Standard (PCI DSS) [requirements](#). However, you can adjust these default settings.

### Workarounds for using SAT and complying with PCI DSS:

- [PCI DSS requirement 8.5.3: Requires users to reset their passwords to a unique value upon first use](#). On the SAT User Settings Template (e.g., **EFTAdhoc**) **Security** tab, clear the **Force users to change their first-time password immediately upon first use** check box.
- [PCI DSS requirement 8.5.9: Change user passwords at least every 90 days](#):
  - On the SAT User Settings Template (e.g., **EFTAdhoc**) **Security** tab, you should disable the **Force user to change their first-time password** check box password reset option. This will also disable the password expiration options for all users on this Settings Template. (Clearing the **Allow users to reset their passwords** check box also clears the **Force users to change their first-time password** check box.)



- o If the SAT administrator password expires or changes, the value stored in the SAT module's configuration file will no longer be valid. This means that each time the SAT-generated administrator account password expires and then is reset, you would have to change the password on the SAT administrator page. Therefore, on the Server's **Administration** tab, click the SAT administrator account, then click **Password Policy** and in the **Password Security Settings** dialog box, clear the **Expire passwords** check box.



**i** If your EFT Server Site's complex password settings require more than 20 characters, be sure to configure the **EFTAdHoc** User Settings Template in EFT Server to override the EFT Server Site's password complexity settings so that complex passwords for SAT temporary users contain fewer than 20 characters. Refer to [Enforcing Strong \(Complex\) Passwords](#) in the EFT Server help for details of creating complex passwords.

When you make these changes on a PCI DSS-enabled ("strict security settings") Site, the **PCI DSS Violations Detected** dialog box appears. Click **Apply this change anyway**, then in the **Provide justification or describe compensating control** box, paste text similar to the following example:

Ad hoc accounts are short-lived accounts with a unique (PCI DSS §8.5.3) and complex (PCI DSS §8.5.10,11) system-generated password. The need to "change after first use" is obviated by the autonomous nature in which the password was generated, as opposed to traditional methods in which an administrator creates a "first time" use password for a user, with its obvious security implications.

## Specifying Virtual Folders for SAT Users

If you would like to store temporary users' folders on a remote computer, you can configure that in EFT Server's Virtual File System (VFS) so that when a file is sent, the temporary user's home folder is created at the location you specified for the Virtual Folder. 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 SAT and IIS are installed must have permission to write to that folder.

For details of specifying the Virtual folder, refer to "Specifying Virtual Folders for SAT Users" in the EFT Server help documentation.



## Using the SAT Module

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

### Sending Files

---

-  *SAT v2 defaulted to anonymous authentication. If you upgraded from SAT v2 to SAT v3, this will be unchanged. For new installs of SAT v3, NT authentication is now standard. In order to send emails, you must have an account on the computer from which you are attempting to send a message and must be a member of the "User's" group.*
- 

#### To send a file using Secure Ad Hoc Transfer

1. Connect to the SAT Send Mail page: In your web browser, provide the IP address or domain name to the IIS website running the Secure Ad Hoc Transfer module, depending on the website and Virtual Folder you chose during installation. For example, type `192.168.20.156/EFTAdHoc` or `www.eftheadhoc.com`. (Or from the **Start** menu, click **Programs > GlobalSCAPE > Secure Ad Hoc Transfer Module > Secure Ad Hoc Send Page.**)

The Send Mail page appears.

-  *If the send mail page does not appear, verify that Java JRE 1.6 or later is running on the client (sender/user) system.*
- 

If the web page 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. When Windows Authentication is used (the default), SAT obtains the corresponding user's e-mail address from the Active Directory account and populates the **From** field with that address.

-  *If the "From" address is disabled, it is because SAT is using your Active Directory provisioned e-mail address, and you are not allowed to specify an alternate from/sender address, for security reasons.*
- 

3. In the **To** box, type the destination address (the intended recipient). If you have sent mail from this page before, addresses you used previously were stored in a cookie. As you type an address, SAT will automatically suggest addresses that you've used before. 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**. (To hide the boxes, click **Show Cc & Bcc** again.) Type the destination address (the intended recipient). You can use the **Cc** and **Bcc** boxes just as you do the **To** box. You can add multiple addresses separated by commas, e.g., `email1@bcd.com, email2@fsr.com`.

-  *SAT limits the **To**, **From**, and **CC** field length to 2048 characters, truncating characters that exceed the limit.*
- 

5. If you want to send a copy of the message your e-mail address, click **Send me a blind carbon copy**.
6. If you want the recipient to be able to send you files, select the **Allow recipient to send me back files**, which enables upload permissions to the temporary folder created for the recipient.
7. (Optional) In the **Subject** box, type the topic of the e-mail.
8. (Optional) In the **Body** box, type a message.

9. Click **Add Attachments** to attach one or more files to the e-mail. (Attachments are not required if **Allow recipient to send me back files** is selected).
  - 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.
10. At the bottom of the page, a file browser appears. Click **Select file(s)/folder(s)** to browse for and select one or more files or folders to attach. The filename, size, and date of each file appears in the file browser. The number of files selected for upload appears in the status bar.
11. To remove attachments, right-click the attached file, then click **Remove selected item(s)** or **Remove all items**.
12. Click **Send**.
  - EFT Server creates a temporary account username and password for the recipient, and then uploads the files.
  - The transfer percent completed appears in the status bar as the files are uploaded.
  - "Uploaded completed" appears in the status bar and a "Complete" message box appears when the transfer is complete.
  - Recipients receive a message notifying them of the files to be picked up, the URL from which to pick up the files, and login credentials information.

## 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 login credentials information.

### To pick up a file

1. In the e-mail, click the hyperlink.
2. In the login page that appears, provide your login credentials, then click **OK**.
  - If using the Web Transfer Client:
    - To download a file, double-click the file in the remote pane to transfer it to your local files and folders.
    - To upload a file, double-click the file in the local pane to transfer it to the remote file system.
  - If using the Plain Text Client, a list of files available for download appears.
    - To download a file, click a file name.
    - To upload a file, click **Browse**, click a file to upload, then click **Upload**.

Refer to the EFT Server online help for more information about the Web Transfer Client or Plain Text Client.

## 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. In version 6.1 and later, 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. In version 6.1 and later, 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. In version 6.1 and later, 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. In version 6.1 and later, 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. In version 6.1 and later, if a user sent multiple files on one e-mail via the SAT module, each of the files are listed in the report.

For details of creating and viewing reports of SAT activity, refer to documentation for the Auditing and Reporting Module.



## Troubleshooting Errors in the SAT Module

Refer to the articles below for troubleshooting assistance.

### 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.

Verify the values supplied for configuration in the SAT [Administration](#) pages. If you are unable to connect to the SAT **Administration** pages (e.g., <http://localhost/EFTAdhoc/admin/>) ensure the settings in the configuration file in the SAT installation folder are correct (by default, **C:\inetpub\wwwroot\EFTAdhoc\config\settings.config**).

Refer to [SAT Module Application Error Codes](#) for any codes that appear on the error page.

### Application Error: Unable to retrieve e-mail address from AD

If you receive an application error that says, "Secure Ad Hoc Transfer (SAT) was unable to retrieve your e-mail address from the Activity Directory server or the e-mail address is invalid," the SAT administrator should verify the [AD Settings](#) in the SAT administration interface.

### SAT Module Application Error Codes

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

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

Error	Description
10001	Not enough disk space to upload the files on drive {0} strTempFolderName
10003	The system could not save files to temporary directory
10006	The caller does not have the required permission to create the specified path (LogPath).
10007	The caller does not have the required permission to create the specified path (IISUploadFolder).
10008	The caller does not have the required permission to delete the uploaded File in the temporary directory.
10009	Unhandled Web exception. Refer to the log files for details.
10010	Unhandled exception. Refer to the log files for details.
10011	Failed to instantiate CIServer. Ensure <b>SFTPCOMInterface.dll</b> is registered on the application server.
10012	Could not initiate connection to EFT Server.
10013	The Site name {0} defined in the configuration file cannot be found on EFT Server.
10014	The temporary user cannot be created on Site {siteName} of the EFT Server. Most likely cause: SAT was installed on an AD or LDAP Site, which cannot create temporary users. Reinstall SAT on a GS or ODBC Site so that EFT Server can create the temporary users.
10015	Failed to set permissions for temporary user on Site {siteName} of EFT Server
10016	Could not get a reference to the temporary user on Site {siteName} of EFT Server
10017	Could not set user home directory as root folder for Temporary user on Site {siteName} of EFT Server
10018	Failed to set expiration date for temporary user on Site {siteName} of EFT Server
10019	Failed to reset permissions for a temporary user on Site {siteName} of EFT Server
10020	Failed to send message by e-mail. Refer to log files for details. (Often caused by the SMTP server being unavailable.)

Error	Description
10021	Expired Version
10022	Failed to instantiate ClientFTPEngineClass. Ensure <b>ClientFTPComLib.dll</b> is registered on the Application Server.
10023	Failed to get retrieved Settings Template for the <b>EFTAdHoc</b> Setting Template. Ensure the <b>EFTAdHoc</b> Settings Template was created on EFT Server. Refer to the log files for details.
10024	Complex password for the user could not be created on Site {siteName}
10025	Change password for the user could not be created on Site {siteName}
10026	Could not set New Full Name for the user.
10027	Access to the path is denied. Refer to the log files for details.
10028	Internal error has occurred; SAT cannot contact the Active Directory Services. Sometimes occurs when the AD server is not operational.
10029	<p>Internal error has occurred; Failed to deliver the payload to the temp account folder. This can be caused by one of the following errors:</p> <ul style="list-style-type: none"> <li>• IIS does not have permission to place the file(s) in the temp account folder.</li> <li>• The end user's home folder drive ran out of space or the physical folder does not exist. The log file will read: "An exception has occurred while moving the payload. Error: {0} StackTrace: {1}"</li> <li>• The physical destination path is greater than 250 characters. The log file will read: "Files cannot be delivered due to the Path '{0}' because the Fullname is greater than 250 characters. Please change the SAT User Setting physical path on EFT Server to use a shorter path."</li> </ul>

# Index

## A

Access Control Policy .....	25
Activating Secure Ad Hoc Transfer .....	17
Active Directory .....	25, 34, 43
Activity-SAT .....	41
Activity-SAT By Recipient .....	41
AD .....	34
AD Extensions .....	43
Adding Blacklist and Whitelist Domains .....	33
Advanced Settings .....	25
Allow Upload .....	32
Application Error	
Unable to retrieve e-mail address from AD ..	43
Auditing .....	41

## B

Background Color .....	29
Banner Image .....	29
BEFORE Installing the SAT Module with IIS7 ...	9
BlackListDestinationDomain .....	25
brand .....	29

## C

Complex Passwords for Temporary Users .....	35
Configuration Pages .....	25
configure .....	25, 35, 43
Configuring Temporary User Account Expiration	
.....	32
Configuring Temporary-User Account Policy ...	32
Configuring the Secure Ad Hoc Transfer Module	
.....	25
Configuring the Secure Ad Hoc Transfer Module	
v3 .....	25
Customizing .....	29
Customizing the Notification E-Mail .....	31
Customizing the Secure Ad Hoc Transfer Web	
Interface .....	29

## D

Default Template Locations .....	35
DefaultPermissionMask .....	25
Delaying the Password Notification E-Mail .....	25
Disable .....	25

## E

EFTAdHoc .....	25
EmailBehavior .....	25
EmailTemplateFormat .....	25
Enforcing Strong (Complex) Passwords .....	35
error .....	43
error codes .....	43
Expirydays .....	25

## F

Failed to Connect to EFT Server .....	43
From .....	43

## H

Header_Logo .....	29
HTML .....	34

## I

IIS .....	7, 25
IIS 7.0 .....	9
IIS7 .....	7
installing .....	10
Installing Secure Ad Hoc Transfer .....	7, 10
Introduction to Secure Ad Hoc Transfer .....	5

## L

LockFromField .....	25
LogLevel .....	25
LogPath .....	25

## M

mailFiltering .....	25
---------------------	----

## N

NET .....	7
Notification E-Mail .....	31
Notify Sender .....	21

## P

Password Notification E-Mail .....	31, 33
PasswordEmailOffset .....	25
PCI Site .....	35
Picking Up Files .....	40
Plain Text .....	34
Populate .....	25

## R

Register- Click Register .....	18
Reporting .....	41

## S

sAMAccountName .....	25
SAT Activity .....	41
SAT Event Rules .....	21
SAT Module Application Error Codes .....	43
SearchFilter .....	25
Secure Ad Hoc Send Page .....	39
Secure Ad Hoc Transfer System Requirements	7
Send Mail .....	43
SenderEmailDisplayAttribute .....	25

Sending a File Using Secure Ad Hoc Transfer 39

Sending Files .....39

SendMail .....29

SendPassword .....25

SendUploadNotification.....21

SendUserName.....25

SetFromFieldWithEmail .....25

settings.config .....25

Single-Click Authentication .....33

SMTPAuthenticate .....25

SMTPServer.....25

SMTPServerPort .....25

Specifying HTML or Plain Text E-Mail Format.34

Specifying Virtual Folders in EFT Server for Ad Hoc users.....37

SystemEmail .....25

**T**

Temporary Account Policy .....32

TempUserNameLength.....25

Troubleshooting Errors in the Secure Ad Hoc Transfer Module .....43

**U**

uninstallation .....23

Uninstalling the SAT Module.....23

upgrading .....18

Upgrading Secure Ad Hoc Transfer.....18

Upload .....21, 40

UploadEFTServerAddress ..... 25

UploadPermissionMask ..... 25

UploadPort ..... 25

URLPattern ..... 25

userPrincipalName..... 25

UseSmartEmailTextBoxes ..... 25

Using SAT with Active Directory ..... 34

Using the HS Module with the Secure Ad Hoc Transfer Module ..... 35

Using the Secure Ad Hoc Transfer Module ..... 39

**V**

VFS ..... 37

Viewing Reports of SAT Activity ..... 41

Virtual Folders for Ad Hoc Users ..... 37

**W**

WaitForUploadsDurationSecs ..... 25

Web Server ..... 7

What's New in Secure Ad Hoc Transfer ..... 5

Whitelist ..... 33

WhiteListDestinationDomain..... 25

Windows 2008 ..... 7

Windows Server 2003..... 7

**X**

x86-64 ..... 7