

GlobalSCAPE[®] EFT Server, v6.1

*Quick Start Guide for EFT Server Interoperability
with Cisco Unified Communications Manager*

GlobalSCAPE, Inc. (GSB)

Corporate Headquarters

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/>

© 2009 GlobalSCAPE, Inc. All Rights Reserved

December 14, 2009

Contents

- Introduction 4**
 - System Requirements for EFT Server..... 4
- Step 1: Download the Software..... 4**
- Step 2: Install EFT Server 5**
- Step 3: Configure the Server 5**
- Step 4: Create a Site and Configure the SFTP Connection 5**
- Step 5: Configure the Cisco Unified Communications Manager for Use with EFT Server 6**
- Getting Help..... 7**
- Windows-Specific Procedures 8**
 - Creating a Windows User Account..... 8
 - Create/Edit Windows Registry Keys for TCP/IP Performance Tuning 12

Introduction

Cisco Unified Communications Manager enables administrators to use SFTP servers for various functions, including to store system backups, send call detail records (CDRs) and call management records (CMRs) to 3rd-party billing servers, send trace and log files from a Cisco Unified Communications Manager server to another server on the network, and to access files during software installation and upgrades. The topics below provide instructions for installing and configuring EFT Server to interoperate with Cisco Unified Communications Manager versions 5.1.x and 6.1.x. You can use either EFT Server basic edition or EFT Server Enterprise. You need the SFTP (SSH2) module to work with Cisco's CUCM. The SFTP module is included in EFT Server Enterprise and is available as a separately licensed module for EFT Server basic edition.

Have this Quick Start Guide and EFT Server's [online help](#) open or [printed out](#) so that you can perform each of the steps in order as described in this guide.

System Requirements for EFT Server

- For a complete list of system requirements for EFT Server and each of its modules, refer to http://help.globalscape.com/help/eft6-1/System_Requirements_for_Server.htm.

For more information about EFT Server:

- For instructions for adding user accounts and other EFT Server configuration procedures, refer to the in-application help or the online help at <http://help.globalscape.com/help/eft6-1/>.
- Request a trial serial number or purchase EFT Server configured for Cisco Unified Communications Manager interoperability at <http://www.globalscape.com/downloads/>.
- For more information about GlobalSCAPE's EFT Server, refer to <http://www.globalscape.com/eft/>.

Step 1: Download the Software

GlobalSCAPE's download page, <http://www.globalscape.com/downloads/>, provides information and links for requesting a trial serial number or purchasing EFT Server. The SFTP (SSH2) module is included in EFT Server Enterprise and is available as a separate module with EFT Server basic edition. (The module is included in the 30-day trial in both EFT Server and EFT Server Enterprise.)

EFT Server Enterprise – Trial Request

Complete the form below and a GlobalSCAPE specialist will contact you with pricing and trial software details. To talk to an account representative, call **1-800-290-5054** (US and Canada) or **1-210-308-8267** (International) M-F, 8-5 US Central time.

* Product Interest:

* First Name:

* Last Name:

* Email Address:

* Phone Number:

* Company:

* Country:

* State or Province:

Questions or Comments:

By filling out this form you agree to allow GlobalSCAPE to contact you. For more information please see our [Privacy Policy](#)

After you complete the purchase or trial form and provide your contact information, the serial number and download link are emailed to you automatically. Follow the instructions in the email to download the software, then install and configure EFT Server as described below.

Step 2: Install EFT Server

Refer to [Installing EFT Server, Administrator, and Modules](#) for complete installation instructions. After installation is complete, you will be asked to login to create a new administrator connection (the Server object) using the credentials that you created during installation. After you log in, click **Continue Trial**. You can activate EFT Server and its modules later.

EFT Server and the SFTP module can be enabled and used during the 30-day trial without a separate license. The SFTP module is included in the EFT Server Enterprise license. If you purchased EFT Server basic edition with the SFTP module, you will also need to activate the SFTP module license when you activate EFT Server. Refer to [Activating the Software](#) for instructions for activating EFT Server and the modules.

Step 3: Configure the Server

After you click **Start Trial**, the EFT Server Setup Wizard appears. Follow the instructions in the wizard and in [Configuring EFT Server](#).

Step 4: Create a Site and Configure the SFTP Connection

After the Server is configured, the Site Setup Wizard appears. SFTP is [enabled at the Site level](#). Follow the instructions in the wizard and in [Defining Connections to EFT Server](#). During the wizard, on the Protocols page, you will need to configure the SFTP port, create or specify the SFTP keys, and specify the SFTP options (encryption algorithms and message integrity algorithms) to be used by the Site.

The Settings Template inherits the settings that you defined on the Site, and the users inherit the settings from their Settings Template, but you can enable SFTP and specify SFTP authentication options separately for Settings Templates and user accounts. Refer to [Configuring SFTP Authentication Options for a Settings Template or User Account](#) for details.

If you do not want to allow FTP connections, clear the FTP check boxes on the Site's **Connections** tab. Refer to [Configuring FTP Transfers on the Site](#) for details.

Refer to the EFT Server help documentation to configure secure [remote administration](#) of the Server, [add users](#) and [permission Groups](#), [define automated event rules](#), and [generate reports](#).

Step 5: Configure the Cisco Unified Communications Manager for Use with EFT Server

Refer to the appropriate Cisco Unified Communications Manager documentation, as described below, for information about configuring SFTP servers in Cisco Unified Communications Manager applications.

The following documents are available at the following link:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

- *Cisco Unified Serviceability Administration Guide*—Describes how to send CDRs and CMRs to 3rd-party billing servers.
- *Disaster Recovery System Administration Guide*—Describes how to store system backups.
- *Cisco Unified Real-Time Monitoring Tool Administration Guide*—Describes how to download trace and log files.
- *Cisco Unified Communications Operating System Administration Guide*—Describes how to access upgrade file during the upgrade process to newer versions of Cisco Unified Communications Manager.

The following documents are available at the following link:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html.

- *Installing Cisco Unified Communications Manager*—Describes how to access upgrade files during the installation process.
- *Upgrading to Cisco Unified Communications Manager from Cisco Unified Communications Manager 4.x Releases*—Describes how to access the Data Migration Assistant TAR file and upgrade files during an upgrade from supported Cisco Unified Communications Manager 4.x releases

Getting Help

For fast answers to most questions, please visit the [GlobalSCAPE Help Center](#). Our Customer Service team can answer your questions about software activation and registration or help with order problems. If you need technical assistance with your software, please submit your question to the [Technical Support](#) team.

- The GlobalSCAPE [User Forum](#) is a great place to find information or seek help from the global community of GlobalSCAPE customers and product experts.
- The GlobalSCAPE [Knowledge Base](#) (KB) is a dynamic compendium of information on our products.
- [Subscribe to the RSS feed](#) to keep abreast of the latest KB articles. Copy and paste this URL <http://kb.globalscape.com/rssfeed.aspx> into your RSS feed reader. (See [below](#) for examples.)
- [Subscribe to GlobalSCAPE E-Mail Announcements](#) Sign up for the GlobalSCAPE Newsletter, press releases, product announcements, and other GlobalSCAPE news.
- [Recover a Lost Serial Number](#) - If you know the e-mail address you used when you activated the software, we can send it to you at your new address.
- [Contact Customer Service](#) by phone or e-mail.
- [Contact Sales](#) by calling 1-800-290-5054 or 1-210-308-8267, or use the online submission form. Sales representatives are available 8:00 a.m. to 6:00 p.m. (US Central Time) Monday through Friday, excluding [major US holidays](#).
- [Order Status](#) - Complete the online e-mail form to request information about your order.
- [Support pages](#) provide downloads, documentation, activation instructions, and the latest news regarding GlobalSCAPE products.

Windows-Specific Procedures

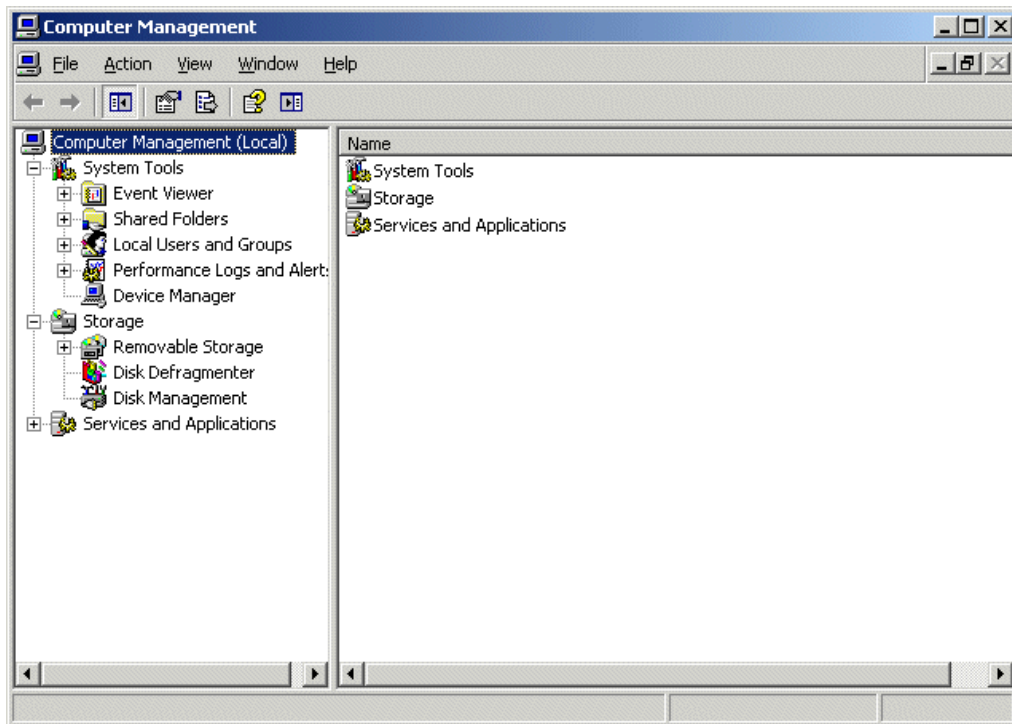
The information below is provided to assist you with configuring Windows to provide more security on the computer on which EFT Server is installed. **It is not necessary to perform these procedures to use EFT Server with the Cisco Unified Communications Manager.** When discussing with your network administrator or IT department the best way to secure your system, keep in mind that EFT Server needs to run as a Local Service, Network Service, or Local System account, and might need access to network resources.

Creating a Windows User Account

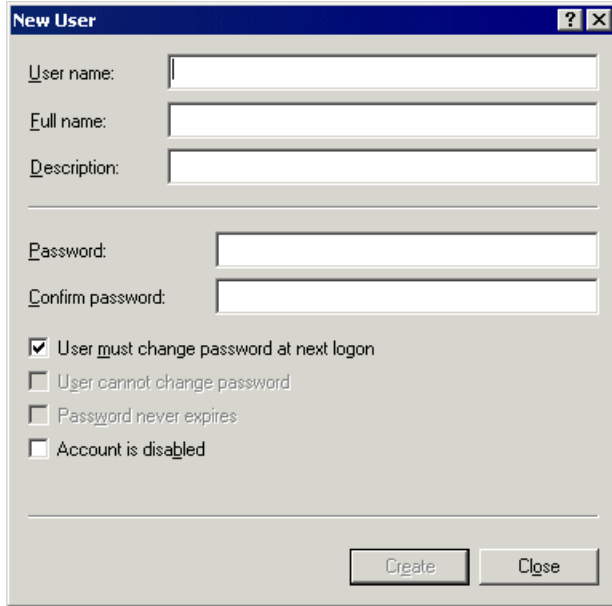
To secure the computer on which the Server is installed, create a Windows user account for the Server and grant **restrictive** permissions to that user account. Setting up a user account increases security, but is not required to run the Server.

To create a user account

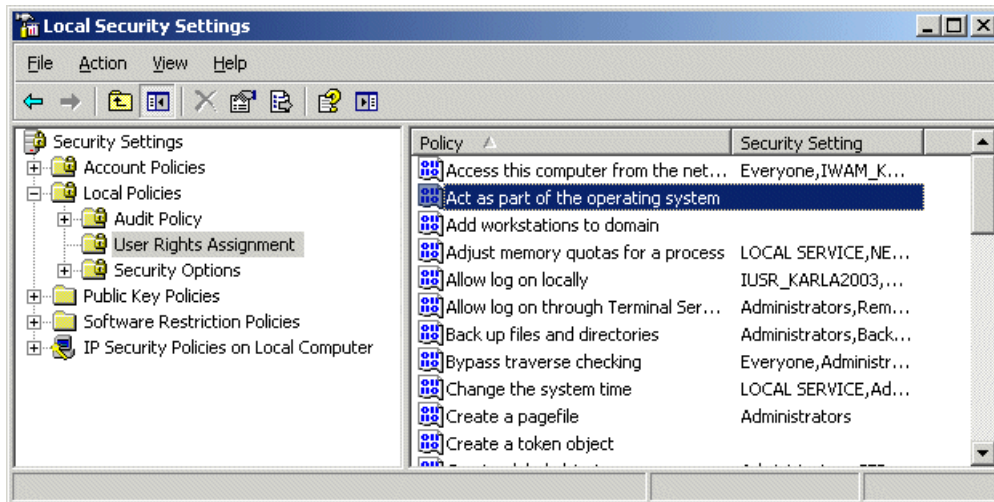
1. After you install the Server, on the desktop, right-click **My Computer**, then click **Manage**. The **Computer Management** console appears.



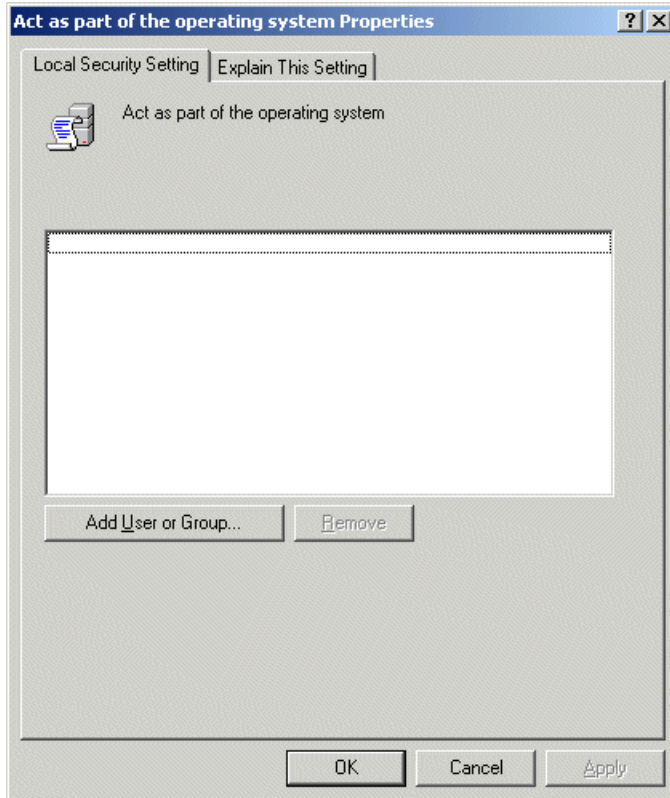
2. Expand the **Local users and groups** node, right-click **Users**, then click **New User**. The **New User** dialog box appears.



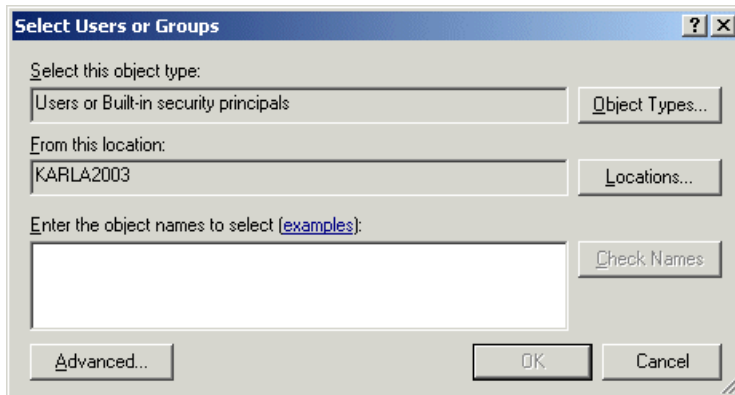
3. Create the user account (user name, password, etc.) click **Create**, then click **Close**.
4. Close the **Computer Management** console.
5. In **Administrative Tools (Start > Run > control admintools)**, double-click **Local Security Policy**. The **Local Security Settings** dialog box appears.
6. Expand the **Local Policies** node, then click **User Rights Assignment**.



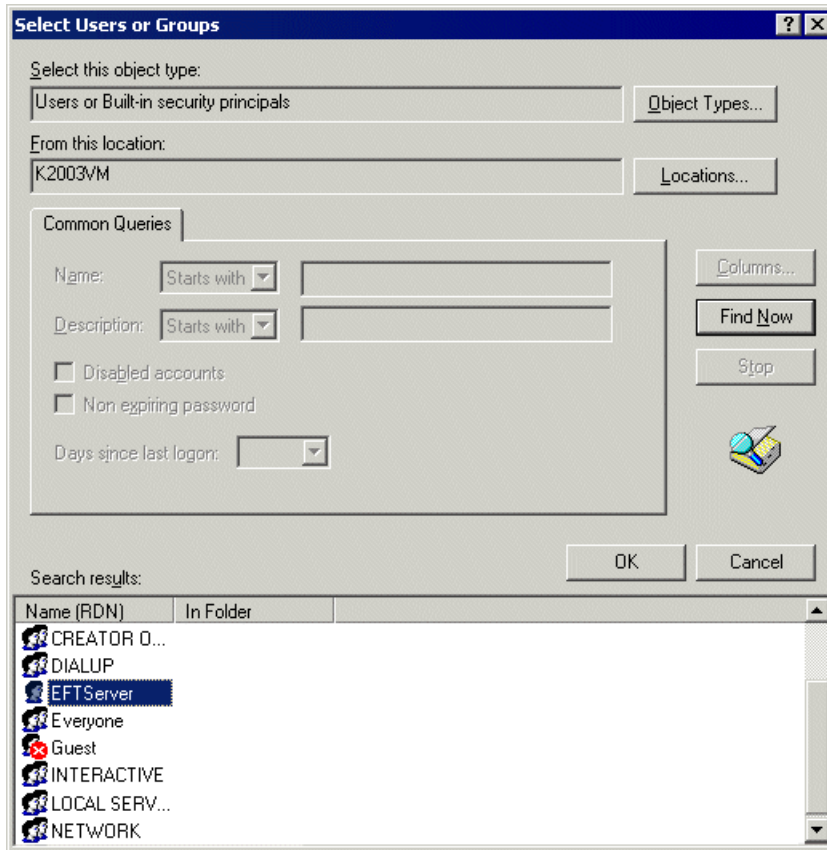
7. In the right pane, in the **Policy** column, double-click **Act as part of the operating system**. The **Properties** dialog box appears.



8. Click **Add User or Group**. The **Select Users or Groups** dialog box appears.



9. Click **Advanced**, then click **Find Now**. The dialog box expands and displays the new user account that you just created (**GSFTPS**).



10. Select EFT Server's account (e.g., **EFTServer**), click **OK** to collapse the **Advanced** box, then click **OK** to save the changes.
11. Open the Windows **Services** dialog box (**Start > Run > services.msc.**)
12. Right-click the EFT Server service, then click **Properties**.
13. Click the **Log On** tab, then follow the Windows operating system procedures for selecting an account under which the service will run.

Create/Edit Windows Registry Keys for TCP/IP Performance Tuning

This topic describes how to tune Windows for TCP/IP performance. It is not necessary to perform these procedures to use EFT Server with the Cisco Unified Communications Manager, and only needed in cases of extremely high traffic on the Server.

To add a key to the registry, you can either edit it directly as described below or create and execute a **.reg** file. When you have finished adding or editing these registry keys, you will need to restart the Server. Configure the following settings or variables below according to your specific tuning needs. If necessary, refer to the GlobalSCAPE Knowledge Base article [Q10411 - HOWTO: Windows Registry Settings](#), for the procedure for creating/editing keys and creating a **.reg** file.



Editing the Windows Registry is for advanced users only. Incorrectly editing the registry can severely damage your system. You should always back up (export a copy of) the registry before you make any changes to it.

TcpTimedWaitDelay

This key determines the time that must elapse before TCP/IP can release a closed connection and reuse its resources. This interval between closure and release is known as the TIME_WAIT state or twice the maximum segment lifetime (2MSL) state. During this time, reopening the connection to the client and server costs less than establishing a new connection. By reducing the value of this entry, TCP/IP can release closed connections faster and provide more resources for new connections. Adjust this parameter if the running application requires rapid release, the creation of new connections, or an adjustment because of a low throughput caused by multiple connections in the TIME_WAIT state.

For more information, refer to the Microsoft MSDN article [TCP TIME-WAIT Delay](#).

To activate this feature, create the following key:

Subkey: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP\Parameters

Value name: TcpTimedWaitDelay

Value data: 0x0000001e (Hex 0x0000001e = decimal 30. This value sets the wait time to 30 seconds.)

MaxUserPort

This key determines the highest port number that TCP/IP can assign when an application requests an available user port from the system.

To activate this feature, create the following key:

Subkey: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP\Parameters

Value name: MaxUserPort

Value data: (minimum) 32768

MaxConnect Backlog

These keys, if many connection attempts are received simultaneously, increase the default number of pending connections that are supported by the operating system.

To activate this feature, create the following 4 keys:

Subkey: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters

Value name: EnableDynamicBacklog

Value data: 00000001

Value name: MinimumDynamicBacklog

Value data: 00000020

Value name: MaximumDynamicBacklog

Value data: 00001000

Value name: DynamicBacklogGrowthDelta

Value data: 00000010

These values request a minimum of 20 and a maximum of 1000 available connections. The number of available connections is increased by 10 each time that there are fewer than the minimum number of available connections.

KeepAliveInterval

This key determines how often TCP repeats keep-alive transmissions when no response is received.

To activate this feature, create the following key:

Subkey: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters

Value name: KeepAliveInterval

Value data: 1 (second)

TcpMaxDataRetranmission

This key determines how many times TCP retransmits an unacknowledged data segment on an existing connection.

To activate this feature, create the following key:

Subkey: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

Value name: TcpMaxDataRetransmissions

Value data: 5 (seconds)

TPC/IP acknowledgements

TCP/IP can be the source of some significant remote method delays. You can increase TCP performance by immediately acknowledging incoming TCP segments, in all situations.

To activate this feature, create the following key:

On Microsoft Windows 2000:

Subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\

Value name: TcpDelAckTicks

Value data: 0

On Microsoft Windows XP, Windows Server 2003/2008:

Subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\

Value name: TcpAckFrequency

Value data: 1