EFT Server™ Configuration Validation

Below is a collection of suggestions and guidelines for installing, configuring, and deploying the Server and/or DMZ Gateway software in a production environment. For a PDF checklist for Security Best Practices, refer to: http://help.globalscape.com/help/eft6-3/mergedProjects/eft/SecurityBestPracticesCheckList.pdf

Development Lab Environment

As with any mission-critical software or hardware, it is recommended that a testing, validation, development, or usability lab be established to provide a "sandbox" into which EFT Server and DMZ Gateway Server software can be deployed. This initial deployment allows for validation of the interoperability with other dependent components as well the validation of expected usage scenarios.

The lab environment should emulate (if not duplicate) the production environment at a network topography and application level. To do this, a clear vision of the production network and the proposed deployment of EFT Server and DMZ Gateway must exist. Typical deployments of EFT Server and DMZ Gateway consist of many other components from the enterprise, including Active Directory Server, SQL Server, SMTP Server, and a storage system such as a *SAN*. For DMZ Gateway, a firewall such as Microsoft *ISA* might be applicable. Finally, some deployments also include Clustering, in which case various components are replicated to provide clustered resources.

For increased business continuity and risk mitigation, you should use the development lab environment as the starting point for any configuration changes in the system. That is, make the change in development and validate it prior to making the change in production.

A good testing tool is CuteFTP Professional.

Configuration Checklist

The installation and configuration of EFT Server in either a lab or a production environment should be validated by EFT Server administrators/operators to ensure that the functions are working as expected. Use the checklist below to validate key items for a Server and DMZ Gateway deployment. Print a PDF of the table below to check off items as you test. (You need Acrobat Reader to open the PDF.) Also refer to the section below this table for Security Best Practices.

Service	
☐	Make sure that the GlobalSCAPE Server service is started on the computer.
☐	Make sure that the service is listening on the expected IP:PORT socket addresses on EFT Server. (To view the listening sockets, use "netstat -ona" from a command line or an application such as PrcView or TcpView.)
☐	Check the Event Viewer log to ensure that there are no errors in the Application log related to EFT Server or DMZ Gateway Server.
☐	Confirm that the administration interface shows the status of the system when it is launched and connected to EFT Server.
Server User Management	
☐	For each Site on EFT Server, ensure that the expected user accounts exist.
☐	To ensure that authentication is working as expected, attempt to log in to EFT Server as a user account on the system (using any protocol).
☐	To confirm that permissions for the user account are working as expected, attempt a file transfer.
Protocol/Network	
☐	For each protocol enabled on EFT Server, attempt a connection directly to EFT Server using a client that supports that protocol.
☐	For each protocol enabled through DMZ Gateway, attempt a connection to the appropriate DMZ Gateway IP:PORT and confirm that this route works as expected.
Auditing/Logging	
☐	View the audit traces generated by the validation steps above.
☐	Confirm that the Auditing and Reporting module database has been populated with appropriate data (using either EFT

	Server Reporting interface or direct access to the SQL Server being used).
☐	Confirm that the text log files generated by EFT Server have been populated with the appropriate data.
Event Rules/Workflow Each customer has a unique set of Event Rule/workflow requirements, but these are the general validation steps. Confirm the following are working as expected:	
☐	**E-mail notifications**. Test e-mail notifications by triggering an Event Rule that has an e-mail notification Action to confirm that Event Rules fire and that the SMTP configuration is correct.
☐	**PGP operations.** Confirm that OpenPGP keys are configured properly.
☐	**Move/Copy/Download actions.** Initiate Event Rules that perform remote file uploads/copies/download so that connectivity originating from EFT Server to a remote system is properly configured. In this step, also confirm that a log file is generated that audits outbound connection information (a "cl*.log" file in the designated Server Log File location).
☐	**Custom Commands**. EFT Server is responsible for triggering those external commands, so that is what should be validated with respect to EFT Server. Any actions carried out by those external tools should be validated independently. Confirm that a "CMDOUT.LOG" file is generated as the result of an invoked Custom Command.
☐	**Folder Monitor Rules.** Ensure that the Event Rules are properly enabled and responsive to files added to the folder being monitored.
Cluster/Failover Testing	
☐	For cluster deployments, the failover and failback operations of the cluster should be confirmed. After a failover/failback, confirm that the newly active server behaves properly; that is, the failover is transparent and the configuration/operation is as expected. This can be summarized by the prior set of tests operating against the newly active node in the cluster.
Load Testing	
☐	If you expect high volumes of traffic or back-end processing within EFT Server, you should verify that the resource utilization levels on EFT Server are within acceptable tolerances. There are numerous load-testing tools available, ranging from simple batch files running command-line FTP to highly complex synthetic transaction generators. GlobalSCAPE's Quality Assurance team performs load testing of our servers as part of our standard validation process for releasing software and can provide guidance and/or tools to assist in load testing.

Numerous other features can be validated within EFT Server. The above set of checks represents the key elements that are most often used and are the most critical to successful operation in a production environment.

For detailed procedures, refer to the online Help topic at:
http://help.globalscape.com/help/eft6-3/index.htm#best_practices_for_configuration_and_validation.htm