DMZ GATEWAY® v3.5
Installation, Administration, and User Guide
<table>
<thead>
<tr>
<th>GlobalSCAPE, Inc. (GSB)</th>
<th>Corporate Headquarters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address:</strong></td>
<td>4500 Lockhill-Selma Road, Suite 150, San Antonio, TX (USA) 78249</td>
</tr>
<tr>
<td><strong>Sales:</strong></td>
<td>(210) 308-8267</td>
</tr>
<tr>
<td><strong>Sales (Toll Free):</strong></td>
<td>(800) 290-5054</td>
</tr>
<tr>
<td><strong>Technical Support:</strong></td>
<td>(210) 366-3993</td>
</tr>
<tr>
<td><strong>Web Support:</strong></td>
<td><a href="http://www.globalscape.com/support/">http://www.globalscape.com/support/</a></td>
</tr>
</tbody>
</table>

© 2008-2019 GlobalSCAPE, Inc. All Rights Reserved

*February 6, 2019*
# Table of Contents

Introduction to DMZ Gateway® .......................................................................................................................... 6
What’s New in DMZ Gateway®? .......................................................................................................................... 7
System Requirements for DMZ Gateway v3.x.................................................................................................... 8
Enabling DMZ Gateway in EFT ............................................................................................................................ 9
DMZ Gateway Technical FAQ ............................................................................................................................ 12
DMZ Gateway Knowledgebase Articles .............................................................................................................. 14
Installing DMZ Gateway ....................................................................................................................................... 15
  Activating DMZ Gateway ................................................................................................................................ 15
  Licensing DMZ Gateway for EFT Enterprise with the Accelerate Module ................................................. 15
  Activation Interaction between DMZ Gateway and EFT Trial ..................................................................... 16
Frequently Used Commands (non-Windows) .............................................................................................. 17
Initialization and Connection Diagrams ......................................................................................................... 20
Installing DMZ Gateway on a Windows System ........................................................................................... 25
Installing DMZ Gateway on a non-Windows System ....................................................................................... 29
  Installing DMZ Gateway on RedHat or SuSE Linux 32-Bit or 64-Bit ...................................................... 29
  Installing DMZ Gateway on Ubuntu Linux 32-Bit or 64-Bit ..................................................................... 30
  Solaris x86 32-Bit or 64-Bit .......................................................................................................................... 31
  Example of Installation Process ...................................................................................................................... 32
  Manually Registering and Deregistering the DMZ Gateway Daemon (non-Windows Systems) .......... 33
  Uninstalling DMZ Gateway on a Windows System ................................................................................ 35
  Uninstalling DMZ Gateway on a non-Windows System ..................................................................... 35
  Upgrading or Repairing DMZ Gateway ....................................................................................................... 36
Administering DMZ Gateway ............................................................................................................................. 38
  Allow LDAP Authentication to EFT through DMZ Gateway ............................................................... 38
  Controlling Access by IP Address ............................................................................................................... 42
  Creating a Profile ............................................................................................................................................ 43
  Default Network Ports for EFT and DMZ Gateway ............................................................................... 45
  Deleting a Profile ........................................................................................................................................... 48
# The DMZ Gateway Interface

DMZ Gateway Administration Interface PID File

DMZ Gateway Components

DMZ Gateway Server

DMZ Gateway Server Service

DMZ Gateway Administration Interface

DMZ Gateway System Files

DMZ Gateway Headless Administration

X11 Server Method

Manual Configuration Method

DMZ Gateway Logging

DMZ Gateway Communications Activity Logging

DMZ Gateway Server Diagnostics Logging

DMZ Gateway Server Service Diagnostics Logging

DMZ Gateway Statistics Logging

DMZ Gateway Server Event Viewer (Windows Operating Systems Only)

DMZ Gateway Server Syslog (Solaris/Linux-based Operating Systems Only)

DMZ Gateway Administration Interface Logging

DMZ Gateway Server Configuration File (gwconfig.xml) Reference

Configuration Validation

Configuration Elements

File Location

DMZ Gateway Server Unix/Solaris Daemon

DMZ Gateway Status

Error Codes

Editing a Profile

Internal Domain Settings

Renaming a Profile

Routing AS2 Traffic through DMZ Gateway

Specifying the Listening IP Addresses
What Does This Mean for the Peer Server Listeners? ................................................................. 72
What Does This Mean for the Client Listeners? ............................................................................ 72
Specify Whether DNS Lookup is Performed on EFT or DMZ Gateway ........................................... 72
Starting and Stopping the DMZ Gateway Server Service .............................................................. 73
DMZ Gateway Server PID Files ...................................................................................................... 73
DMZ Gateway Server Status Files .................................................................................................. 74
DMZ Gateway Server Monitoring ..................................................................................................... 74
Testing the Configuration ................................................................................................................... 74
Troubleshooting DMZ Gateway Communication ............................................................................. 75
Using DMZ Gateway as an Outbound Proxy .................................................................................... 76
Viewing Statistics .............................................................................................................................. 76
Peer Notification Channels Tab ......................................................................................................... 76
Client Listeners Tab .......................................................................................................................... 77
Statistics Tab ....................................................................................................................................... 78
DMZ Gateway Secure PNC ................................................................................................................ 78
Introduction to Secure PNC .............................................................................................................. 78
Remote Administration of EFT ........................................................................................................... 79
Configuring Secure PNC .................................................................................................................... 80
Configuring Secure PNC using a Self-Signed Certificate ................................................................ 80
Configuring Secure PNC using an EFT Certificate ........................................................................ 80
Secure PNC Settings .......................................................................................................................... 85
Secure PNC Logging .......................................................................................................................... 86
Interface Reference ........................................................................................................................... 87
IP Access Exception Entry Dialog Box .............................................................................................. 87
New Profile Wizard - Profile name ..................................................................................................... 88
New Profile Wizard - Peer Server Access .......................................................................................... 88
New Profile Wizard - Configuration .................................................................................................... 89
Introduction to DMZ Gateway®

DMZ Gateway® is designed to reside in the demilitarized zone and provide secure communication with a server behind intranet firewalls without requiring any inbound firewall holes between the internal network and the DMZ, and with no sensitive data stored in the DMZ, even temporarily. DMZ Gateway supports connections to EFT using Profiles. Depending on the license purchased, you can have up to 15 Profiles (unique IP address:port connections).

How Does It Work?

1. When the EFT service is started, it will establish (and maintain) an outbound connection to the DMZ Gateway. This proprietary, non-encrypted connection is called the Peer Notification Channel (PNC). EFT and DMZ Gateway use the PNC to setup subsequent communications between EFT and incoming client connections.

2. When a client (web browser, FTP client, etc.) connects to DMZ Gateway on a pre-approved port (21, 22, 80, 443, etc.), DMZ Gateway will cross reference the client’s IP with the IP access list (provided by EFT over the PNC) before proceeding any further.

3. If the IP is accepted, DMZ Gateway will notify EFT over the PNC of the new client connection, providing data such as the client’s IP address and the port to which they are connected.

4. EFT will subsequently create a new outbound connection to the DMZ Gateway to the same port that is being used by the PNC for associating with the client connection made in step 2.

5. DMZ Gateway will then proceed to read the inbound payload data from the client and send the payload data to EFT for processing. DMZ Gateway will also read any outbound data communication from EFT and send it to the client.
The graphic below describes the flow in EFT:

What's New in DMZ Gateway®?

Changes in version 3.5:
- Ability to configure secure PNC for remote administration of EFT
- Updated support for non-Windows operating systems

Changes in version 3.4:
- Released April 25, 2016
- EFT version 7.3.0 and later (Windows OS only)
- Support for EFT with the Accelerate module

The Accelerate module/FAST protocol is not supported on Linux versions of DMZ Gateway.

Changes in version 3.3.1:
- Released December 8, 2014
- EFT v6.5 and later
- Removed support for Windows Server 2003
- Added Business Activity Monitor (BAM) as a recognized server type
• Upgraded the Java Service Wrapper to Version 3.5.19. This version includes an automatic deadlock
detection/restart feature.

Changes in version 3.3.0:

• Released February 15, 2013
• EFT v6.5 and later
• Support for IPv6 addressing when operating with Mail Express version 3.3 and later
• Added support for Unicode strings in the log files and XML-based configuration files
• Added support for Unicode strings in communications with the EFT platform v6.5 and later
• Changed installer so that it now ensures the DMZ Gateway administration interface is not running
  prior to making modifications
• Fixed an issue that prevented binding to interfaces if IPv4 or IPv6 support was disabled in the
  operating system
• Fixed minor user interface issues in the DMZ Gateway administration interface
• Upgraded the embedded Java Runtime Environment to version 1.7.0_09.

System Requirements for DMZ Gateway v3.x

It is possible for DMZ Gateway to function with other operating systems, software, and hardware, but has only
been tested with the systems listed below.

• **EFT and DMZ Gateway cannot** be installed on the same computer/image, but must be installed no more
  than one network “hop” away with an average network latency no greater than 50ms, with zero percent
  packet loss, and normal packet flow. Refer to
  [https://kb.globalscape.com/KnowledgebaseArticle11444.aspx](https://kb.globalscape.com/KnowledgebaseArticle11444.aspx)
  for more information.

• The Accelerate module/FAST protocol is not supported on Linux versions of DMZ Gateway.

• Supported operating systems:
  o Windows Server 2016 (64-bit)
  o Windows Server 2012 R2 (requires GUI component) - 64-bit (there is no 32-bit version)
  o CentOS (latest)
  o Red Hat Enterprise Linux 7.3 64-bit Kernel: 3.10.0-514
  o SuSE Linux Enterprise Server 12.2 64-bit (SP2) (requires you to be logged in as “root” to
    launch the DMZ Gateway administration interface)
  o Ubuntu 16.04.3 LTS
  o Amazon Linux AMI 2017.03.1 64-bit (Admin console is not supported)

• 2 CPUs
- 200 MB hard drive space for the application (No data is ever stored on the DMZ Gateway computer, not even temporarily.)
- 1GB available RAM
- 1280x800 resolution or higher display (headless computer supported on non-Windows systems)
- The DMZ Gateway installer installs the latest Java Runtime Environment (JRE); you do not need to update or maintain the JRE. (The installer uses the latest version at the time the installer is built. Refer to the release notes to see which version was installed.)
- Remote administration must be available.
- DMZ Gateway v3.5 requires EFT v7.4 and later. DMZ Gateway v3.5 will work with EFT v7.3 for basic functionality, but the EFT v7.4-specific features added to DMZ Gateway v3.5 are not available in EFT v7.3.

The command-line parameter `/NOREQS` can be used if installing at a command line. If specified, the installer will skip checking for the minimum OS prerequisite that occurs during initial installer launch. This setting is mainly used for debugging purposes or when the checks have errors that are preventing a valid install in the field. Only check #1 for minimum OS is available for DMZ Gateway. Refer to “Silent Command Line Installation” in the EFT help documentation for more information.

"Internet Protocol Version 4 (TCP/IPv4)" must be installed on the operating system. If you are using "Internet Protocol Version 6 (TCP/IPv6)," "Internet Protocol Version 4 (TCP/IPv4)" may be disabled instead of uninstalled. (In the Local Area Connection Properties dialog box, clear the check box next to "Internet Protocol Version 4 (TCP/IPv4)") It is OK to have them both enabled at the same time.

Enabling DMZ Gateway in EFT

You can enable DMZ Gateway when you create the Site or enable it later in the EFT administration interface. In the Site Setup wizard for both standard and High Security Sites, EFT displays the Perimeter Security configuration page that asks whether you will be using DMZ Gateway, and allows you to enter the DMZ Gateway IP address and port number. If Connect this site to EFT's DMZ Gateway is selected when you are creating a Site in the Site Setup wizard, EFT attempts to establish a socket connection to DMZ Gateway when you click Next.

- If the socket connection fails, a message appears in which you are allowed to provide the DMZ Gateway information again or disable DMZ Gateway and continue without it. (You can attempt to configure it again later.)
- If the socket connection is successful, EFT applies the settings and continues with Site setup.

To enable DMZ Gateway in EFT administration interface

1. In the EFT administration interface, connect to EFT and click the Server tab.
2. Expand the node of the Site you want to connect to DMZ Gateway, then click the Gateway node.
3. In the right pane, the **DMZ Gateway** tab appears.

4. Select the **Enable the DMZ Gateway as a proxy** check box.

5. In the **DMZ Gateway address** box, specify the IP address of the DMZ Gateway to which you are connecting.

6. In the **Port** box, specify the port number over which EFT is to connect to DMZ Gateway. The default port is 44500.

   The connection will be refused if the IP address is on the server's IP Access\Ban list.

7. Select the **Secure (TLS) Peer Notification Channel (PNC)** check box.

8. In the **Protocols** area, select the check boxes for the protocols and the ports that DMZ Gateway will use. These settings are separate from the ports that EFT uses. For example, you could use port 21 for FTP traffic directly to EFT, but port 14421 for FTP traffic through the DMZ Gateway.

9. If you are using DMZ Gateway with a PASV mode IP address, click **PASV settings**. The **Firewall/NAT Routing** dialog box appears.
a. Select the Assign PASV mode IP address check box, then specify the IP address and port range.

b. Click OK.

10. Click **Apply** to save the changes on EFT. If the settings are correct and the DMZ Gateway is configured properly, the connection status changes to **Connected** with a green icon.

```
If EFT cannot connect to DMZ Gateway, ensure that the EFT computer can connect to the DMZ Gateway computer by pinging it. Verify that the DMZ Gateway firewall is not blocking incoming connections.
```

11. You may need to establish a new connection with EFT Server by stopping and restarting connected Sites.

   a. In the left pane, click the Site node.

   b. In the right pane, click the **General** tab.

   c. Click **Stop**. The **Site Status** area displays "Stopped" with a red ball icon.

   d. Click **Start**. The **Site Status** area displays "Running" with a green ball icon.

**Related Topics**

- [Enabling Acceleration](#)
- [DMZ Gateway Secure PNC](#) (Remote administration)
DMZ Gateway Technical FAQ

Below are some frequently asked technical questions about the DMZ Gateway.

**Does DMZ Gateway modify the client’s packets?**

DMZ Gateway effectively terminates the client’s TCP/IP session at the DMZ Gateway. The client data contained within the payload of the TCP/IP packet is transmitted to the server over the independently established TCP/IP connection between the server and DMZ Gateway. No modifications are required or performed on the actual payload data, but rather the payload is sent as is to the server. Thus, if the client is using HTTPS, then the HTTPS payload is streamed on through to the server. Unlike a network hardware bridge/router device, the DMZ Gateway does not “pass through” modified packets by changing the TCP/IP or frame layer headers. Instead, the DMZ Gateway reads in a buffer full of data from the client TCP/IP stream (~64KB) and then sends that data over the TCP/IP socket established earlier by the server (see step 4 above). The result is a set of completely different TCP/IP packets with different source and destination locations but containing the original payload. Keep in mind that the original (source) location (IP address) is known by the server as it was provided to the server earlier by DMZ Gateway (see step 3 above).

**Does DMZ Gateway forward client connections to the server?**

The DMZ Gateway does not forward client connections. Only the payload (data) is forwarded or passed through to the server.

**How do the server’s listening ports affect DMZ Gateway?**

EFT allows you to define two groups or sets of listening ports. When used with DMZ Gateway, the external listening ports (DMZ Gateway Internet facing) are specified in EFT Server’s administration interface on the DMZ Gateway tab. EFT’s second set of listening ports, defined on the Site’s Connections tab, are ONLY used for establishing internal listening ports (server-network facing) for each supported (and enabled) protocol. These sets of ports can be the same or different (even for the same protocol). When DMZ Gateway is NOT being used (i.e., the server is residing in the DMZ or is being used for internal, network-facing transactions), then only a single set of ports is used, defined on the Site’s Connections tab, for all incoming connections to EFT.

**How is the PNC created and maintained?**

Once configured to work with DMZ Gateway, the server (when running) will always attempt to initiate, maintain, and, if necessary, reconnect to DMZ Gateway’s PNC port. No further administrative action is required in the server to establish or maintain communication after the initial setup. From DMZ Gateway’s perspective, if the PNC channel is broken, DMZ Gateway will refuse new (and existing) client connections until the server re-establishes a connection.
The server will “ping” the DMZ Gateway every 5 minutes. If a reply is not received within 10 seconds, the server considers the connection lost, severs the current connection, and then attempts to reconnect. DMZ Gateway also maintains its own awareness (ping/pong) of whether the server is connected. Every 30 seconds, DMZ Gateway determines whether it has received a pong message from the server since the last ping. If it has, it will ping again; if not, it drops the connection. This test allows it to free up ports if the server is not available (i.e., no longer responds to ping) and for error reporting. (Refer to the Knowledge Base article “How do EFT and DMZ Gateway Server communicate with each other?” for information about changing these defaults in EFT 6.2 and later and DMZ Gateway 3.0 and later.)

The PNC between the server and DMZ Gateway is not encrypted; however, the external client’s encrypted session will be streamed all the way through to the server, so only the intercommunications between the server and the DMZ Gateway are in the clear, not the client session (assuming they used a secure protocol such as SFTP or HTTPS). (Refer to DMZ Gateway Secure PNC for information about configuring a secure PNC.)

But won’t an insecure PNC be vulnerable to a man-in-the-middle attack?

In order to usurp the PNC connection, the attacker would need full control over the internal systems on which the server is running. This access would indicate a far greater threat to Confidentiality, Integrity, and Availability (CIA) already in place in your network. Keep in mind that the internal firewall should be configured to allow only outbound connections from the server to DMZ Gateway via the PNC port. If configured as such, then the ability to usurp the control connection doesn’t really gain the attacker much of an edge. Even if a connection were seized, the attacker would need to perform several other non-trivial steps, such as spoofing the server’s IP address*, reverse engineering the protocol, opening ports on the firewall, altering the routing table, etc.

*DMZ Gateway provides an optional whitelist for IP addresses that are allowed to connect to the PNC port. (Refer to DMZ Gateway Secure PNC for information about configuring a secure PNC.)

Isn’t DMZ Gateway just giving users a way to bypass the firewall without providing any security functionality or filtering?

The DMZ Gateway is not designed to replace firewalls or content-inspection devices. The DMZ Gateway’s main purpose is to allow network administrators to minimize the exposure surface area by allowing you to further lock down the internal firewall such that only outbound connections are needed, thus eliminating the need for inbound connections through your internal firewall to your directory server (for user authentication) or SQL/Oracle server (for transaction auditing). Furthermore, it eliminates the need to store file data in the DMZ. Essentially DMZ Gateway limits the attack vector to the server as opposed to multiple other internal servers. As far as filtering is concerned, it is important to note that DMZ Gateway does not replace any other sort of filtering mechanism, such as firewalls, web application firewalls, content inspection devices, and so on. DMZ Gateway is intended to work with and extend existing security mechanisms.
So then, any vulnerability in the server is essentially exposed to the Internet?

Assuming vulnerabilities exist then yes, those would be exposed to the Internet; however, the attack vector would be limited to attacks that could be accomplished over the network protocols that are proxied through the DMZ, as there would be no means for the attacker to establish inbound connections to the server directly, because of the EFT <> DMZ Gateway architecture. (Refer to DMZ Gateway Secure PNC for information about configuring a secure PNC.)

What about Denial of Service attacks? Wouldn’t it be trivial to pump traffic all the way through the DMZ to where EFT resides?

EFT is a file transfer server. It is meant to handle anything you can throw at it over the various listeners. EFT includes a number of DoS and flood-prevention mechanisms to mitigate these sorts of attacks. This would be the same if you stood up EFT (or any other FTP server) in the DMZ and terminated connections there. If EFT Server designates one or more IP addresses as needing to be blocked, it will add those IP addresses to its own internal IP Access Rules list and communicate that list to DMZ Gateway. DMZ Gateway will subsequently block all external clients with blacklisted IP addresses on the access list.

If there is a change to EFT’s IP access rules, are the changes communicated immediately to the DMZ Gateway when those changes are applied?

Yes, IP address access policy changes (whether manually initiated or as a byproduct of an auto-ban) are automatically propagated to the DMZ Gateway (v3.0 and later). (Refer to Remote Administration for information about banning IP addresses with a secure PNC.)

DMZ Gateway Knowledgebase Articles

For further assistance, refer to the following articles in the Globalscape Knowledgebase.

- #10023 - Changing the ping interval
- #10583 - Common questions about the new DMZ Gateway version 3
- #10686 - Connecting to a Remote Host Using DMZ Gateway as a Proxy
- #10710 - Overriding the default Profile limit in DMZ Gateway
- #10865 - Overriding the default Network Access Policy Exception limit in DMZ Gateway
- #10866 - Overriding the default SOCKS5 Connection Security in DMZ Gateway
- #11060 - Why isn’t the Peer Notification Channel (PNC) encrypted?
- #11201 - DMZ Gateway® Configuration Settings
- #11270 - DMZ Gateway® Flood Protection Setting
- #11280 - Activating the Accelerate module
- #11300 - Do I need a multi-site license for DMZ Gateway if I want to use it with EFT SMB/Express and Mail Express?
• #11131 - Failed FTP connection after upgrading DMZ Gateway
• #11114 - Installing or Upgrading DMZ Gateway in a Failover (ACTIVE/PASSIVE) Cluster
• #11205 - Using CuteFTP® with DMZ Gateway® for testing remote EFT™ Connections
• #11206 - Running DMZ Gateway as non-root user in Linux
• #11233 - WebHelp not displaying properly in browser
• #11292 - How to submit a ticket to support
• #11390 - In the IP Access List in EFT, any "banned" IP addresses beyond the first 1000 are not blocked when DMZ Gateway is used.
• #11395 - DMZ Gateway administration interface fails to launch on SuSe Linux

(Check out https://kb.globalscape.com/KnowledgebaseCategory35.aspx often as new articles may have been added since this was published.)

Installing DMZ Gateway

The topics in this section provide instructions for installing DMZ Gateway.

Activating DMZ Gateway

DMZ Gateway licensing is activated in the connecting application, not DMZ Gateway, which accepts connections from any licensed application. For example, a Single-Site license enables one EFT Site to connect to any available DMZ Gateway. A Multi-Site license enables one or more Sites from EFT Enterprise to connect to any available DMZ Gateway. DMZ Gateway allows up to 15 Profile definitions to manage connections, but the license installed on the connecting application determines how many connections are allowed to DMZ Gateway.

After the 30-day trial has expired, you must activate DMZ Gateway by activating the serial number in the connecting application’s administration interface. Refer to the EFT documentation for details of activating DMZ Gateway.

Licensing DMZ Gateway for EFT Enterprise with the Accelerate Module

When licensing DMZ Gateway for EFT Enterprise with the Accelerate module (for Windows only), not only do you have to activate DMZ Gateway (and the Accelerate module) in EFT Enterprise, you also must install a license file in the DMZ Gateway installation directory, as described below, for each DMZ Gateway used.

To activate DMZ Gateways for EFT Enterprise with the Accelerate module

1. Provide your DMZ Gateway server host’s public-facing / forward-facing Internet Protocol (IP) address to your Globalscape point of contact. In return, you will receive two files derived from the supplied IP address:
   • DeiLicense.dat
   • FastImpl.dll
2. On the DMZ Gateway computer, stop the DMZ Gateway server service.

3. In the `lib` folder of the DMZ Gateway installation folder (e.g., `C:\Program Files\GlobalSCAPE\DMZ Gateway\lib`), replace the file FastImpl.dll with a new version provided by Globalscape.

4. In the `conf` folder of the DMZ Gateway installation folder (e.g., `C:\Program Files\GlobalSCAPE\DMZ Gateway\conf`), paste your license file (e.g., `DeiLicense.dat`).

5. Start the DMZ Gateway server service.
   - DMZ Gateway will log the attempted registration and record its success or failure.
   - Registration is maintained upon upgrade or repair.
   - If the DMZ Gateway’s host IP changes, you will need to request a new FastImpl.dll from Globalscape.

**Activation Interaction between DMZ Gateway and EFT Trial**

- When both EFT and DMZ Gateway are in trial mode, all DMZ Gateway features are enabled.
- If the EFT trial period expires (has not been activated) and the DMZ Gateway module has not been activated, EFT will:
  - Halt all outbound Peer Notification Channel (PNC) communication to the DMZ Gateway.
  - Disable all controls on EFT’s DMZ Gateway configuration pages.
  - Disable the **Use EFT Server’s DMZ Gateway as the proxy** check box in the Event Rule **Copy/Move** or **Download Action** wizards’ **Proxy Settings** dialog box, which will cause any Event Rule to fail that uses DMZ Gateway as an outbound proxy.
  - Hide the **Perimeter Network Security** page of the Site Setup wizard in EFT.
  - Write a warning to the Windows Event Log: “EFT Server’s DMZ Gateway module evaluation period has expired.”
- If EFT is activated, but DMZ Gateway is in trial mode, the DMZ Gateway is fully functional until the DMZ Gateway trial expires. Once DMZ Gateway expires, all functionality and controls in EFT are disabled (unless you activate DMZ Gateway).
- If DMZ Gateway is activated using a single–Site serial number:
  - EFT allows only one DMZ Gateway site to be enabled.
  - If more than one DMZ Gateway node was enabled prior to activation, all but one node will be disabled, the PNC of each of the disabled Sites is disconnected, and an error is written to the Windows Event Log: “EFT – One or more DMZ Gateway connections were disabled due to licensing restrictions. Make sure your DMZ Gateway module license matches the number of DMZ Gateway ‘Sites’ enabled. Contact your Globalscape account representative for further assistance.”
- EFT’s COM engine will return an error if you attempt to start a DMZ Gateway when one is already enabled.
- If DMZ Gateway is activated using a multiple-Site serial number, EFT allows up to 15 DMZ Gateways to be enabled (one per EFT Site).

**Frequently Used Commands (non-Windows)**

The table below describes several commands that you use to administer DMZ Gateway on non-Windows platforms. The commands are described in the applicable procedures in more detail; this table is provided only as a quick reference.

In the examples below, *your file and path names may differ.*

- **Install**

  **Platform:** All
  **Example:**
  ```
  gunzip dmz-gateway-linux-x86-32.tgz
  tar xvf dmz-gateway-linux-x86-32.tar
  ./Install.sh
  ```

- **Register the script**

  **Platform:** Redhat
  **Example:**
  ```
  chkconfig --add dmzgatewayd
  ```

  **Platform:** Suse
  **Example:**
  ```
  insserv dmzgatewayd
  ```

  **Platform:** Ubuntu
  **Example:**
  ```
  update-rc.d dmzgatewayd defaults
  ```

  **Platform:** Solaris
  **Example:**
  ```
  ln -sf /etc/init.d/dmzgatewayd /etc/rc0.d/K99dmzgatewayd
  ln -sf /etc/init.d/dmzgatewayd /etc/rc1.d/K99dmzgatewayd
  ```
ln -sf /etc/init.d/dmzgatewayd /etc/rc2.d/S99dmzgatewayd
ln -sf /etc/init.d/dmzgatewayd /etc/rc3.d/S99dmzgatewayd

• **Deregister the script**

  **Platform:** Redhat
  **Example:**
  ```
  chkconfig --del dmzgatewayd
  ```
  **Platform:** Suse
  **Example:**
  ```
  insserv -r dmzgatewayd
  ```
  **Platform:** Ubuntu
  **Example:**
  ```
  rm /etc/init.d/dmzgatewayd
  update-rc.d dmzgatewayd remove
  ```
  **Platform:** Solaris
  **Example:**
  ```
  rm /etc/rc0.d/K99dmzgatewayd
  rm /etc/rc1.d/K99dmzgatewayd
  rm /etc/rc2.d/S99dmzgatewayd
  rm /etc/rc3.d/S99dmzgatewayd
  ```

• **Uninstall**

  **Platform:** All
  **Example:**
  ```
  /opt/dmzgateway/bin/Uninstall.sh
  ```

• **Open the DMZ Gateway Interface**

  **Platform:** All
  **Example:**
  ```
  /opt/dmzgateway/bin/DMZGatewayAdmin
  ```
• **Start DMZ Gateway Server service**

  **Platform:** All

  **Example:**

  /opt/dmzgateway/bin/dmzgatewayd start

• **Stop DMZ Gateway Server service**

  **Platform:** All

  **Example:**

  /opt/dmzgateway/bin/dmzgatewayd stop
Initialization and Connection Diagrams

The diagrams below illustrate the initialization and connection sequences for DMZ Gateway and EFT communication.

DMZ Gateway Peer Notification Channel (PNC) Initialization Sequence

1. EFT initiates a connection to DMZ Gateway’s PNC listener. This connection will serve as the PNC between the connecting EFT site and DMZ Gateway.

2. With the connection established, EFT sends a login request over the new connection that identifies the EFT site and provides its configuration.

3. DMZ Gateway creates client-side (outbound facing) listeners based on the site’s configuration.

4. DMZ Gateway sends a response to the login request completing the PNC handshake.

5. The PNC between the EFT site and DMZ Gateway is established. DMZ Gateway will use the PNC to inform EFT of client connection requests and EFT will use the PNC to make FTP-related outbound connection requests.
DMZ Gateway FTP Command Channel Connection Sequence

1. Client connects to DMZ Gateway using the FTP protocol. The connection is assigned a unique identifier (connection Id).

2. DMZ Gateway notifies EFT of the new client connection request via the FNC. The notification includes the connection Id.

3. EFT responds by creating a new connection to the DMZ Gateway. This connection will be used to broker the new client connection.

4. EFT sends a response notification over the new connection that includes the identifier of the client connection this new connection will service.

5. DMZ Gateway pairs up the client-side and server-side connections using the client connection identifier. The command channel portion of the FTP session is now established. All information sent by the client is forwarded to EFT and vice-versa.
DMZ Gateway FTP Passive Mode (PASV) Connection Sequence

1. Client issues FTP PASV command over command channel.  
   ![Client-side portion of command channel]  
   ![Server-side portion of command channel]  
   ![PNC Connection]

2. EFT responds by creating a new connection to DMZ Gateway. This connection will be used as the server-side portion of the FTP data channel.  
   ![Client-side portion of command channel]  
   ![New Connection]  
   ![Server-side portion of command channel]  
   ![PNC Connection]

3. EFT issues a client-side listen request over the new connection instructing DMZ Gateway on which interface (IP address) it should listen for the client connection. Normally this is the same IP address the command channel is connected to but can be a specific IP address depending on how EFT is configured. The request also instructs DMZ Gateway if it should use a port from a given range or simply choose any ephemeral port (the default).  
   ![Client-side portion of command channel]  
   ![Client-side Listen Request (optional)]  
   ![Server-side portion of command channel]  
   ![PNC Connection]

4. DMZ Gateway responds by sending EFT a notification over the same connection informing it of the local IP address and port on which it will be listening for the data channel connection. DMZ Gateway then begins listening for a connection.  
   ![Client-side portion of command channel]  
   ![Listen Response (192.168.1.100:29000)]  
   ![Server-side portion of command channel]  
   ![PNC Connection]
5. EFT responds to the client PASV command over the command channel. The response includes the IP address and port to which the client should connect in order to establish the data channel.

6. Client initiates a new connection to DMZ Gateway based on the PASV command response.

7. DMZ Gateway notifies EFT that it has accepted the client connection using the connection established for the data channel wrapper.

8. The data channel has now been established. Data sent from the client is now forwarded to EFT and vice versa.
DMZ Gateway FTP Active Mode (PORT) Connection Sequence

1. Client issues FTP PORT command over the command channel specifying the local IP address and port EFT should connect to in order to establish the data channel. In the example this is 192.168.1.100:6000.

2. EFT responds by creating a new connection to DMZ Gateway. This connection will be used as the server-side portion of the FTP data channel.

3. EFT issues a client-side connect request over the new connection instructing DMZ Gateway on which IP address and port it should connect to the client in order to complete the data channel. This is the IP address and port specified by the client in the PORT command.

4. DMZ Gateway connects to the IP address and port specified by the client-side connection request sent by EFT.

5. EFT Server issues a response to the client PORT command to notify the client that the command succeeded.

6. The data channel has now been established. Data sent from the client is now forwarded to EFT Server and vice versa.
Installing DMZ Gateway on a Windows System

DMZ Gateway and the connecting application must be installed on separate computers.

- If you are installing or upgrading DMZ Gateway in a cluster configuration, refer to Installing DMZ Gateway in a Cluster.
- If you are upgrading, refer to Upgrading or Repairing DMZ Gateway.

To install DMZ Gateway

1. Close all unnecessary applications so that the installer can update system files without rebooting the computer.

2. Start the installer. The Welcome page appears.

3. Click Next. The License Agreement appears.
4. Read the license, then click I Agree.

5. If an existing installation is detected, refer to Upgrading or Repairing DMZ Gateway. Otherwise, the Choose Installation Location page appears.

6. The Destination Folder box displays the default location. Keep the default displayed in the box or click Browse to specify a different location. Also displayed is the amount of hard drive space required to install the program.

7. Click Next. The Choose Configuration Location page appears.
8. In the **Configuration Folder** box, specify the path at which to store configuration files for DMZ Gateway. The installation location is specified by default, but you can specify a separate location for backup and disaster recovery or for shared resources, such as with a cluster environment.

9. Click **Next**. The shortcuts page appears.

A shortcut to open the DMZ Gateway interface will be installed on the **Start** menu in a folder called **Globalscape**. You can keep this default location or specify a different location in which to install the shortcut.

10. Click **Install**. The product is installed and the installation log appears.
11. Click Next. The completed page appears.

The **Start the Administration Interface, Create a desktop shortcut, and Start the DMZ Gateway Server service** check boxes are selected by default. Select the **Show version history** check box if you want to read the release notes. (You can also access the release notes in the installation folder.)

12. Click Finish. If you left the **Start the Administration Interface** check box selected, the **DMZ Gateway Administration Interface** appears.

A default Profile is defined that will listen on all IP addresses of the computer on which you installed DMZ Gateway. By default, it will listen for connections from servers on port 44500.

- Refer to **Editing a Profile** to change the IP address/port assignments.
• Refer to Creating a Profile to create new/additional Profiles.
• Refer to Controlling Access by IP Address to specify which IP addresses or IP masks are allowed or denied connections.

Installing DMZ Gateway on a non-Windows System

The installation process on each non-Windows operating system is the same, with a few minor differences. The basic process of installation can be described as follows:

1. Copy the appropriate installer archive file (.tgz) to the target machine.
2. Extract the contents of the installer archive. The archive contains two files: an installation script and an archive of the actual program files.
3. Run the installation script as root and follow the prompts.

The process for supported non-Windows operating systems is described below. (For installation on Windows systems, refer to Installing DMZ Gateway.)

The installation script includes registering and starting the DMZ Gateway server daemon (configuring it to auto-start on system start and auto-stop on system stop). Alternately, you can start the server manually using the command `<InstallDir>/bin/dmzgatewayd start`. Refer to Manually Registering and Deregistering the DMZ Gateway Server Daemon if you decide not to register the daemon during the installation process.

Installing DMZ Gateway on RedHat or SuSE Linux 32-Bit or 64-Bit

To install DMZ Gateway

1. Transfer the appropriate DMZ Gateway Linux installer archive to a convenient directory on the target machine.
2. On the target machine, open a terminal window. The installation package must be run with root privileges. If not already logged on as the root user, change to root using the `su` command in the terminal window:
   ```
su
   ```
3. Change to the directory containing the installer archive and perform the following:

   • On 32-bit systems:
     ```
     gunzip dmz-gateway-linux-x86-32.tgz
tar xvf dmz-gateway-linux-x86-32.tar
     ./Install.sh
     ```

   • On 64-bit systems:
     ```
     gunzip dmz-gateway-linux-x86-64.tgz
     ```
tar xvf dmz-gateway-linux-x86-64.tar
./Install.sh

4. Follow the prompts to complete the installation.
   • You are prompted to accept the license agreement, and to specify the installation and configuration directories (e.g., `/opt/dmzgateway`), etc.
   • After everything is installed, you are prompted to register and start the DMZ Gateway daemon service.
   • If you start the service, you can execute the DMZ Gateway Administration interface script (e.g., type: `/opt/dmzgateway/bin/DMZGatewayAdmin`).

Refer to the example below for details of the installation process.

Installing DMZ Gateway on Ubuntu Linux 32-Bit or 64-Bit

To install DMZ Gateway

1. Transfer the DMZ Gateway installer archive into a convenient directory on the target machine.

2. On the target machine, open a terminal window.

3. Change to the directory containing the installer archive and perform the following:
   • On 32-bit systems:
     - gunzip dmz-gateway-linux-x86-32.tgz
     - tar xvf dmz-gateway-linux-x86-32.tar
     - sudo ./Install.sh
   • On 64-bit systems:
     - gunzip dmz-gateway-linux-x86-64.tgz
     - tar xvf dmz-gateway-linux-x86-64.tar
     - sudo ./Install.sh

4. On 64-bit systems:
   - gunzip dmz-gateway-linux-x86-64.tgz
   - tar xvf dmz-gateway-linux-x86-64.tar
   - sudo ./Install.sh

5. Follow the prompts to complete the installation.
   • You are prompted to accept the license agreement, and to specify the installation and configuration directories (by default: `/opt/dmzgateway`), etc.
   • After everything is installed, you are prompted to register and start the DMZ Gateway daemon service.
   • If you start the service, you can execute the DMZ Gateway Administration interface script (e.g., type: `/opt/dmzgateway/bin/DMZGatewayAdmin`).

Refer to the example below for details of the installation process.
Solaris x86 32-Bit or 64-Bit

To install DMZ Gateway

1. Transfer the appropriate DMZ Gateway installer archive to a convenient directory on the target machine.

2. On the target machine, open a terminal window. The installation package must be run with root privileges. If not already logged on as the root user, change to root using the su command in the terminal window:
   
   su

3. Change to the directory containing the installer archive and perform the following:
   
   - On 32-bit systems:
     
     gunzip dmz-gateway-solaris-x86-32.tgz
     
     tar xvf dmz-gateway-solaris-x86-32.tar
     
     ./Install.sh
   
   - On 64-bit systems:
     
     gunzip dmz-gateway-solaris-x86-64.tgz
     
     tar xvf dmz-gateway-solaris-x86-64.tar
     
     ./Install.sh

4. Follow the prompts to complete the installation.
   
   - You are prompted to accept the license agreement, and to specify the installation and configuration directories (e.g., /opt/dmzgateway), etc.
   
   - After everything is installed, you are prompted to register and start the DMZ Gateway daemon service.
   
   - If you start the service, you can execute the DMZ Gateway Administration interface script (e.g., type: /opt/dmzgateway/bin/DMZGatewayAdmin).

Refer to the example below for details of the installation process.
Example of Installation Process

Below is an example of executing the Install.sh script on a Solaris x86 32-bit computer.

```bash
== License Agreement ==
OMITTED – End-user License Agreement
Do you agree to the above license terms? [yes or no]: yes [ENTER]

== Choose Install Location ==
Please specify the path into which the DMZ Gateway program files will be installed or press "Enter" to accept the default.
Specify installation directory [/[opt/dmzgateway]]: [ENTER]

== Choose Configuration Location ==
Please specify the path to store the DMZ Gateway Server configuration settings or press "Enter" to accept the default.
Specify configuration directory [/[opt/dmzgateway]]: /export/home/appdata [ENTER]

== Choose Installation Owner ==
Please specify the user account name to use as the owner of the installed files.
Specify owner [root]: [ENTER]

== Choose Installation Group ==
Please specify the user group name to use as the group of the installed files.
Specify group [root]: [ENTER]

== Confirm Settings ==
Installation directory: /opt/dmzgateway
Configuration directory: /export/home/appdata
Installation owner: root
Installation group: root
Are these settings correct? [yes or no]: yes [ENTER]

Creating directory "/opt/dmzgateway"
Creating directory "/export/home/appdata"
Unpacking archive...
Extracting files...
OMITTED - Extracted Program File List
Unpacking JRE...
Extracting JRE...
OMITTED - Extracted Java Runtime Environment File List
Removing temporary files...
Updating permissions...
Updating ownership...
Updating configuration file...

== Register Service ==
The installation script can attempt to register the DMZ Gateway Server daemon service (dmzgatewayd) for automatic startup and shutdown.
Register the DMZ Gateway Server daemon service? [yes or no]: yes
Creating symbolic link "/etc/init.d/dmzgatewayd"
Creating symbolic link "/etc/rc0.d/K99dmzgatewayd"
Creating symbolic link "/etc/rc1.d/K99dmzgatewayd"
Creating symbolic link "/etc/rc2.d/S99dmzgatewayd"
Creating symbolic link "/etc/rc3.d/S99dmzgatewayd"

== Start Service ==
The installation script can attempt to start the DMZ Gateway Server daemon service (dmzgatewayd).
Start the DMZ Gateway Server daemon service? [yes or no]: yes [ENTER]
Executing: /etc/init.d/dmzgatewayd start

== Installation Complete ==
The DMZ Gateway is now installed.
The DMZ Gateway Server daemon service may be controlled using the "dmzgatewayd" script:
/opt/dmzgateway/bin/dmzgatewayd
The DMZ Gateway Administration Interface may be started using the script:
/opt/dmzgateway/bin/DMZGatewayAdmin
```
Manually Registering and Deregistering the DMZ Gateway Daemon (non-Windows Systems)

During the installation process, you are prompted to register the DMZ Gateway server daemon (configuring it to auto-start on system start and auto-stop on system stop). If you choose not to register the daemon during the installation process, use the procedure below to add or remove the DMZ Gateway daemon script, dmzgatewayd, from automatic system startup and shutdown.

There are multiple methods of configuring a daemon script for automatic startup/shutdown on Linux/Solaris. Ultimately, whatever method is used typically results in the creation of symbolic links in the /etc/rc* directories. These scripts are called at different startup and shutdown run levels of the operating system to start and stop the daemon.

RedHat Enterprise Linux

After creation of the /etc/init.d/dmzgatewayd symbolic link, the `chkconfig` command can be used to register and deregister the script for system startup/shutdown.

To register the script

- The following command may be used as root:
  
  ```bash
  chkconfig --add dmzgatewayd
  ```

  (there are two dashes before add)

To deregister the script

- The following command may be used as root:
  
  ```bash
  chkconfig --del dmzgatewayd
  ```

  (there are two dashes before del)

SuSE Linux

After creation of the /etc/init.d/dmzgatewayd symbolic link, the `insserv` command can be used to register and deregister the script for system startup/shutdown.

To register the script

- The following command may be used as root:
  
  ```bash
  insserv dmzgatewayd
  ```

To deregister the script

- The following command may be used as root:
  
  ```bash
  insserv -r dmzgatewayd
  ```
Ubuntu Linux

After creation of the `/etc/init.d/dmzgatewayd` symbolic link, the `update-rc.d` command can be used to register and deregister the script for system startup/shutdown.

To register the script

- The following command may be used as root:
  ```
  update-rc.d dmzgatewayd defaults
  ```

To deregister the script

- The `/etc/init.d/dmzgatewayd` symbol link must first be removed using the following command as root:
  ```
  rm /etc/init.d/dmzgatewayd
  ```

To deregister the daemon

- The following command may be used as root:
  ```
  update-rc.d dmzgatewayd remove
  ```

Solaris

On Solaris, after creation of the `/etc/init.d/dmzgatewayd` symbolic link you typically manually create the appropriate symbolic links in the `/etc/rc*` directories.

To register the script

- The following commands may be used as root:
  ```
  ln -sf /etc/init.d/dmzgatewayd /etc/rc0.d/K99dmzgatewayd
  ln -sf /etc/init.d/dmzgatewayd /etc/rc1.d/K99dmzgatewayd
  ln -sf /etc/init.d/dmzgatewayd /etc/rc2.d/S99dmzgatewayd
  ln -sf /etc/init.d/dmzgatewayd /etc/rc3.d/S99dmzgatewayd
  ```

To deregister the script

- Remove the symbolic links as root:
  ```
  rm /etc/rc0.d/K99dmzgatewayd
  rm /etc/rc1.d/K99dmzgatewayd
  rm /etc/rc2.d/S99dmzgatewayd
  rm /etc/rc3.d/S99dmzgatewayd
  ```
Uninstalling DMZ Gateway on a Windows System

Uninstall DMZ Gateway using Windows’ Add/Remove Programs tool or via the shortcut on the Start menu.

Uninstalling DMZ Gateway on a non-Windows System

The installation process on each non-Windows operating system is the same with a few minor differences. The basic process of installation can be described as follows:

• Run the uninstallation script as root and follow the prompts. (The script is created during installation and is <InstallDir>/bin/Uninstall.sh)

RedHat Enterprise Linux, SuSE Linux, or Solaris x86 32-Bit or 64-Bit

You can uninstall DMZ Gateway using the Uninstall.sh script located in the <InstallDir>/bin directory.

To uninstall DMZ Gateway

1. On the target machine, open a terminal window. The uninstall script must be run with root privileges.
   If not already logged on as the root user, change to root using the su command in the terminal window:
   su
2. Run the Uninstall.sh script:
   /<InstallDir>/bin/Uninstall.sh
   For example:
   /opt/dmzgateway/bin/Uninstall.sh
3. Follow the prompts to complete uninstalling.

Ubuntu Linux 32-Bit or 64-Bit

You can uninstall DMZ Gateway using the Uninstall.sh script located in the <InstallDir>/bin directory.

To uninstall DMZ Gateway on Ubuntu Linux

1. On the target machine, open a terminal window.
2. Run the Uninstall.sh script:
   sudo /<InstallDir>/bin/Uninstall.sh
   For example:
   sudo /opt/dmzgateway/bin/Uninstall.sh
3. Follow the prompts to complete uninstalling.
Example of Uninstallation Process on Solaris

The following is a sample execution of the Uninstall.sh installation script run on Solaris x86 32-bit.

--- Confirm Uninstallation ---
The uninstallation script will now uninstall the DMZ Gateway from the following installation directory:
/opt/dmzgateway
Proceed with uninstallation? [yes or no]: yes [ENTER]

--- Stop Service ---
The installation script has detected that the DMZ Gateway Server daemon service (dmzgatewayd) is currently running. The service must be stopped before proceeding. The script can now attempt to stop the service.
Stop the DMZ Gateway Server daemon service? [yes or no]: yes [ENTER]
Executing: /etc/init.d/dmzgatewayd stop Stopping DMZ Gateway Server... Stopped DMZ Gateway Server.

--- Deregister Service ---
The installation script can attempt to deregister the DMZ Gateway Server daemon service (dmzgatewayd) from automatic startup and shutdown.
Deregister the DMZ Gateway Server daemon service? [yes or no]: yes [ENTER]
Removing /etc/init.d/dmzgatewayd symbolic link...
Deregistering system daemon:
rm /etc/rc0.d/K99dmzgatewayd rm /etc/rc1.d/K99dmzgatewayd rm
/etc/rc2.d/S99dmzgatewayd rm /etc/rc3.d/S99dmzgatewayd
Removing installation files...

--- Uninstallation Complete ---

Upgrading or Repairing DMZ Gateway

Upgrades from version 2.x to version 3 of the DMZ Gateway are supported on Windows systems only. You must upgrade DMZ Gateway before upgrading EFT.

To upgrade or repair DMZ Gateway on non-Windows systems

- Perform the standard installation process for the target operating system and use the same settings for installation path and configuration path. If the DMZ Gateway Server daemon service is running, you are prompted to stop it; if you do not stop it, the installer will abort.

To upgrade on Windows systems

1. Close the administration interface.

2. As a precaution, back up the existing installation directories and any other files you may have installed elsewhere.

3. Launch the installer and then click Next. The License Agreement appears.

4. Click I Agree. The installer will detect an existing installation.

5. The older version must be uninstalled. You can keep the existing configuration or use the (new) default configuration. Click one of the following, then click Next:
   - Keep existing configuration and uninstall the older version
   - Use a default configuration and uninstall the older version

6. Follow the prompts to finish the upgrade. Refer to Installing DMZ Gateway, if necessary.

   During the upgrade process, the DMZ Gateway service Log On As account is set to use the Local System account.
To upgrade from DMZ Gateway 3.x on Windows systems

1. Close the administration interface.
2. Launch the installer. The installer will detect an existing installation.
3. After accepting the End-User License Agreement, click **Upgrade DMZ Gateway**, then click **Upgrade**.
4. Follow the prompts to finish the upgrade. Refer to *Installing DMZ Gateway*, if necessary.

To reinstall DMZ Gateway 3.x on Windows systems

Reinstallation can be used to fix installations in situations where program files have been corrupted or accidentally deleted. During reinstallation, the installer will reinstall the original copies of corrupted or missing program files.

1. Close the administration interface.
2. Launch the installer. The installer will detect an existing installation.
3. After accepting the End-User License Agreement, click **Reinstall DMZ Gateway**, then click **Reinstall**.
4. Follow the prompts to finish the reinstall. Refer to *Installing DMZ Gateway*, if necessary.
Administering DMZ Gateway

The topics in this section provide instructions for administering DMZ Gateway.

Allow LDAP Authentication to EFT through DMZ Gateway

Suppose an EFT administrator wants to create an environment in which users in their internal network (as specified by their LDAP server) can access the server to do whatever they want; however, they do NOT want those employees to visit the server from outside their own offices. They also have Workspaces participants that are outside the company, and they need to distinguish INTERNAL access from EXTERNAL access. Described below is a way to set a host name for their DMZ Gateway (internet facing) entry to EFT, and anything flowing into EFT from that path will be considered EXTERNAL. Allowing LDAP authentication to EFT through DMZ Gateway is only for directly signing into WTC (not clicking Workspace in a notification email).

(See also Specifying External and Internal Domains and Internal Domain Settings dialog box in Site configuration.)

Hyperlinks in Workspaces notification emails are composed based upon recipient domain:

- External Users will be directed towards the domain address on the site-connections tab
- Internal Users will be directed towards the address on the internal domain button of the DMZ Gateway

The external domain is specified on the Site’s Connections tab:
An Internal Domain is specified on the DMZ Gateway tab:

![DMZ Gateway settings interface]

Hyperlinks in notification emails are composed based upon recipient domain:

- In the DMZ Gateway tab Internal Domain settings, the internal email domain list, similar to email domain list in Workspaces Drop-Off tab, is, by default, empty. Empty means no email domain matching is performed and links are not altered.

- In the DMZ Gateway tab Internal Domain settings, the internal host name is, by default empty. Empty means that no domain matching is performed and links are not altered.

- If EFT sends an email where the email domain (after the "@" symbol) matches one of the specified "internal domains" values, any URLs formed by EFT and pointing to EFT in the email should be constructed using the internal host name (e.g., mft2go.internal.com).

- If no internal host name was specified, then EFT will use the default host name.

- If EFT sends an email where the email domain (after the "@" symbol) matches NONE of the specified "internal domains" values, any URLs formed by EFT and pointing to EFT in the email should be constructed using the default host name specified in the DMZ Gateway tab.
To specify the internal domain on an LDAP site

1. In the EFT administration interface, click the **Server** tab, then click the **Gateway** node.
2. On the **DMZ Gateway** tab, next to the **HTTPS** port box, click **Internal Domain.** The **Internal Domain Settings** dialog box appears.

![Internal Domain Settings dialog box](image)

Only invitation emails sent to these domains will include this alternate link address. All others will point to the default links.

3. In the **Internal host name** box, specify the URL through which internal users should log in to EFT.
4. Click **Configure** to specify the SSL certificate settings.
5. In the **Internal email domain(s)** box, specify one or more SMTP domains used by internal users, separated by semicolons.
6. (optional) To allow internal LDAP accounts to authenticate to EFT through DMZ Gateway, select the **Allow LDAP authentication to EFT through DMZ Gateway** check box. (Cleared by default.)
7. (optional) To allow LDAP authentication available only for internal accounts, select the **Make LDAP authentication exclusive for internal connections** check box. (Cleared by default.)
8. (optional) To enable two-factor authentication for internal domain users, select the **Require 2nd factor auth for internal users** check box. (Cleared by default.)
9. Click **OK**.

To specify a custom LDAP attribute to populate user's email at Site and Settings Template level

1. On the LDAP Site's **General** tab, click **Configure.** The **LDAP Authentication Options** dialog box appears.
2. Click **Advanced.** The **LDAP Authentication Advanced Options** dialog box appears.
Custom Attributes:

- Multiple attributes can be added to each custom field, but only the first attribute will be used; All other attributes will be ignored.
- An attribute field on the LDAP server can contain multiple attributes if you want multiple attributes added to a single custom field (example: address)

If a user account has been removed from EFT due to inactivity, the user can still log in to Workspaces. The account will be added back to EFT after they log in.
Controlling Access by IP Address

By default, all IP addresses are granted access to DMZ Gateway. You can grant access to only one specific IP address or a range of IP addresses, or deny access to one specific address or a range of addresses. You can define up to 100 IP address masks.

For example, if you want to allow only 192.168.174.159 and block every other IP address, click **Denied access**, click **Add**, then type 192.168.174.159 in the **IP mask** box. This will deny access to all IP addresses except 192.168.174.159.

To grant/deny access by IP Address

1. In the Profile tree, click the default **Profile** or [create a new profile].
2. In the **Configuration** pane, click the **Access** tab. The exception list appears.
3. The **Access** tab displays the IP addresses that are granted or denied access. By default, all IP addresses are granted access, and no exceptions are displayed in the list.
4. To configure exceptions, click **Granted access** or **Denied access**.
   - If most IP addresses are **allowed access**, click **Granted access**, then add the exceptions (IP addresses that are not allowed access).
   - If most IP addresses are **denied access**, click **Denied access**, then add the exceptions (IP addresses that are allowed access).
5. Click **Add**. The **New IP Access Exception Entry** dialog box appears.
6. Specify the IP address or range of IP addresses to which you are denying or granting access. You can use wildcards to select ranges of IP addresses.
7. Click **OK**. The IP address/mask appears in the exceptions list.
8. Click **Apply Changes** to save the changes on DMZ Gateway.
Creating a Profile

Creating a Profile includes specifying the listening IP address for incoming clients, specifying the listening IP addresses and port for the connecting application, and specifying the IP addresses that are allowed or denied access.

To create a Profile

1. Do one of the following:
   - Right-click in the Profiles tree, then click **New Profile**.
   - On the toolbar, click **New Profile**.
   - On the main menu, click **Profile > New**.

   The **New Profile Wizard** appears.

2. In the **Profile Name** box, provide a unique name for this Profile. The name will appear in the interface, logs, error messages, and reports.

3. Click **Next**. The **Configuration** page of the wizard appears.
4. In the Listening IP for incoming Clients box, click the down arrow to select one or more IP addresses for incoming clients. Refer to Specifying the Listening IP Addresses for details.

5. In the Listening IP for Server box, click the down arrow to select one or more listening IP addresses for the server. Refer to Specifying the Listening IP Addresses for details.

6. In the Port box, provide the port number over which connections are allowed.

   The connection will be refused if the IP address is on the IP address ban list.

7. If you are using the Accelerate module in EFT, specify the Listening IP for Acceleration.


9. All IP addresses are granted access by default. To grant or deny access to specific IP addresses (optional):

10. Click Granted access or Denied access.

    o If most IP addresses are allowed access, click Granted access, then add the exceptions.

    o If most IP addresses are denied access, click Denied access, then add the exceptions.
For example, if you want to allow only 192.168.174.159 and block every other IP address, click **Denied access**, click **Add**, then type 192.168.174.159 in the **IP Mask** box. This will deny access to all IP addresses except 192.168.174.159.

11. Click **New**. The **New IP Access Exception Entry** dialog box appears.

12. Specify the IP address or range of IP addresses to which you are denying or granting access. You can use wildcards to select ranges of IP addresses.

13. Click **OK** to close the **New IP Access Exception Entry** dialog box.

14. Click **Finish**. The IP Mask appears in the exception list.

**Default Network Ports for EFT and DMZ Gateway**

The table below provides information about the default network ports used for clients (i.e., browsers and web clients) and services such as AS2 and web services.

<table>
<thead>
<tr>
<th>Ports</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| TCP: 443 (HTTPS) | **Inbound**: Encrypted web connections for transferring files with EFT used by clients (browsers, web clients) and the services such: AS2, Mobile Transfer Client. Invoke event rules via Web Services. EFT account management (password changed).  
**Outbound**: Encrypted web connections used by EFT to transfer files via HTTPS with other application servers. |
| TCP: 80 (HTTP)   | **Inbound**: Unencrypted web connections to transferring files with EFT used by clients (browsers, web clients) and other application servers.  
**Outbound**: Unencrypted web connections used by EFT to transfer files via HTTP with other application servers. |
| TCP: 22 (SFTP)    | **Inbound**: Encrypted TCP connections for transferring files with EFT via SFTP protocol used by SFTP clients.  
**Outbound**: Encrypted TCP connections used by EFT to transfer files via SFTP protocol with other SFTP servers. |
| TCP: 21 (FTP)  | **Inbound**: Unencrypted or Encrypted (Explicit SSL) TCP connections for transferring files with EFT via FTP protocol used by FTP clients. |
### EFT File Transfers protocols

<table>
<thead>
<tr>
<th>Ports</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| TCP: 990/ (FTP Implicit SSL) TCP: 989 (outbound) | **Outbound**: Unencrypted or Encrypted (Explicit SSL) TCP connections used by EFT to transfer files via FTP protocol with other FTP servers.  
**Inbound**: Encrypted TCP connections for transferring files with EFT via FTP protocol used by FTP clients.  
**Outbound**: Encrypted TCP connections used by EFT to transfer files via FTP protocol with other FTP servers. |
| TCP: 29000-30000 (FTP using PASV) | **Inbound**: Unencrypted or Encrypted TCP connections for transferring files with EFT via FTP when using PASV mode by FTP clients. |

### EFT Management, Notifications, and Auditing and Reporting

<table>
<thead>
<tr>
<th>Ports</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP: 1100 (Administration Port)</td>
<td>TCP Unencrypted or Encrypted (SSL/TLS) connection used by EFT to manage its configuration via EFT Admin console or SFTPCOMInterface API</td>
</tr>
<tr>
<td>TCP: 4450 (HTTPS)</td>
<td>Port used by EFT as an Administration REST API, used by EFT Insight for manage and gather configuration from EFT.</td>
</tr>
<tr>
<td>TCP: 1433 (SQL Server)</td>
<td>TCP Unencrypted or encrypted (SSL/TLS) connection used to save and retrieve ARM logs into SQL Server</td>
</tr>
</tbody>
</table>
| TCP: 1521 (Oracle)  
TCP: 2484 (Oracle SSL) | TCP Unencrypted or encrypted (SSL/TLS) connection used to save and retrieve ARM logs into SQL Server |
| TCP: 25465, 587 (SMTP) | TCP unencrypted connections used by EFT protocol for sending email notifications via SMTP. |
| TCP: 143 (IMAP)  
TCP: 993 (IMAP SSL) | TCP unencrypted or encrypted (SSL) connections used by EFT for sending email notifications via IMAP. |

### EFT Content Integrity Control

<table>
<thead>
<tr>
<th>Ports</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP: 1344 (ICAP)</td>
<td>Unencrypted or encrypted (SSL/TLS) HTTP connection used by EFT to communicate with an ICAP server protocol for DLP (e.g. virus scanning, content filtering).</td>
</tr>
</tbody>
</table>

### DMZ Gateway

<table>
<thead>
<tr>
<th>Ports</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP: 44500</td>
<td>TCP Unencrypted or encrypted (SSL/TLS) connections used by EFT to connect to, control DMZ and transfer files from DMZ gateway.</td>
</tr>
<tr>
<td>UDP: 8443</td>
<td>Port used by DMZ gateway to connect to another DMZ using FAST protocol for file transfers using the accelerate transfer module.</td>
</tr>
</tbody>
</table>
## EFT File Transfers protocols

<table>
<thead>
<tr>
<th>Ports</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Storage</strong></td>
<td></td>
</tr>
<tr>
<td>Direct TCP: 445 NetBIOS UDP: 137,138 NetBIOS TCP: 138,139</td>
<td>SMB/CIFS protocol used by EFT to connect to a file shares (NAS) as a backend data storage</td>
</tr>
<tr>
<td>TCP: 860, 3260</td>
<td>iSCSI ports typically used by SAN storage, and consumed by EFT as storage presented as a NTFS local drive or file shares.</td>
</tr>
<tr>
<td>UDP: 138</td>
<td>DFS, Group Policy and NetBIOS used for Storage replication if used by EFT Server</td>
</tr>
<tr>
<td><strong>EFT High Availability</strong></td>
<td></td>
</tr>
<tr>
<td>TCP: 1801 RPC: 135, 2101*, 2103*, 2105* UDP: 3527, 1801</td>
<td>Message Queuing default ports used by EFT to operate when deployed in High Availability mode and maintain its configuration synchronized and load balance processing of event rules. UDP ports used when EFT is configured as multicast.</td>
</tr>
<tr>
<td><strong>Active Directory</strong></td>
<td></td>
</tr>
<tr>
<td>Active Directory TCP: 135</td>
<td>RPC protocol used by Microsoft for Active Directory replication</td>
</tr>
<tr>
<td>UDP: 67</td>
<td>DHCP Server</td>
</tr>
<tr>
<td>TCP 139</td>
<td>User and Computer Authentication, Replication, DFSN, NetBIOS Session Service, NetLogon</td>
</tr>
<tr>
<td>TCP and UDP: 53</td>
<td>User and Computer Authentication, Name Resolution, Trusts</td>
</tr>
<tr>
<td><strong>LDAP</strong></td>
<td></td>
</tr>
<tr>
<td>TCP and UDP: 389</td>
<td>LDAP Directory, Replication, User and Computer Authentication, Group Policy, Trusts</td>
</tr>
<tr>
<td>TCP: 3268</td>
<td>LDAP Global catalog for Directory, Replication, User and Computer Authentication, Group Policy, Trusts</td>
</tr>
<tr>
<td>TCP: 3269</td>
<td>LDAP Global catalog for Directory, Replication, User and Computer Authentication, Group Policy, Trusts</td>
</tr>
</tbody>
</table>
### EFT File Transfers protocols

<table>
<thead>
<tr>
<th>Ports</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Authentication</td>
<td></td>
</tr>
<tr>
<td>Ports</td>
<td>Purpose</td>
</tr>
<tr>
<td>TCP: 1812</td>
<td>RADIUS server default port used by EFT for multifactor authentication</td>
</tr>
<tr>
<td>TCP: 4400 (HTTPS)</td>
<td>Encrypted HTTPS connections used by EFT to Authenticate users with the Identity Provider Server using SAML protocol</td>
</tr>
</tbody>
</table>

#### Deleting a Profile

You can configure multiple Profiles. You can delete Profiles that you no longer use, but you cannot delete a Profile if it is the only Profile.

**To delete a Profile**

- Click the Profile in the tree, then do one of the following:
  - Right-click the Profile name, then click **Delete Profile**.
  - On the toolbar, click **Delete Profile**.
  - On the main menu, click **Profile > Delete Profile**.

The Profile is deleted from the tree.

#### The DMZ Gateway Interface

The DMZ Gateway interface is used for mapping and viewing DMZ Gateway connections. **Profiles** are used to define connections to DMZ Gateway.

**To open the interface**

- On Windows systems, double-click the DMZ Gateway shortcut on the desktop or **Start** menu.
- On non-Windows systems, after the server service has started, execute the DMZ Gateway administration interface script (e.g., `/opt/dmzgateway/bin/DMZGatewayAdmin`). On SuSe Linux, you must be logged in as root to launch the administration interface.
- The left pane displays each of the defined **Profiles** in an expandable/collapsible tree view. DMZ Gateway has a default Profile for which you define the listening IP address(es) and port for the connecting application, listening IP address(es) for connecting clients, and the IP address ban list. When DMZ Gateway connects, only the default Profile is displayed. The interface displays the configuration for the last Profile modified or viewed the last time the interface was opened or the first (default) Profile if no “last viewed” profile value is available.
- In the default view, with **All Profiles** selected, the right pane displays the status of the DMZ Gateway service and the status of all Profiles.
• When a Profile is selected, the right pane displays the configuration information and status of the selected Profile.

DMZ Gateway Administration Interface PID File

When the DMZGatewayAdmin executable is launched it will create the PID file `<Installation Directory>\DMZGatewayAdmin.pid`. This file contains the PID for the administration interface process. The timestamp of the file is updated every 10 seconds while the administration interface is running. When the application exits gracefully, it deletes the PID file.

This file is also used to prevent simultaneous execution of multiple copies of the administration interface. When the administration interface starts, it checks for the presence of the PID file. If the file exists and its timestamp has been updated in the last 20 seconds it will assume another copy of the user interface is running and exit.

Related Topics

• Refer to Creating a Profile for information about Profile configuration.
• Refer to Controlling Access by IP Address for information about granting or denying access to a specific IP addresses or an IP mask.
• Refer to Starting and Stopping the DMZ Gateway Server Service for details of stopping and starting the DMZ Gateway server service.
• Refer to Viewing Statistics for details of each of the tabs in the Status pane.
DMZ Gateway Components

DMZ Gateway consists of the following components:

- The main server component, the DMZ Gateway Server
- A launch and monitoring component, the DMZ Gateway Server Service
- A configuration and monitoring component, the DMZ Gateway administration interface

DMZ Gateway Server

The DMZ Gateway Server is the main Java-based functionality. An embedded Java Runtime Environment (JRE) is used to execute this functionality. (The JRE is installed with DMZ Gateway—you do not need to install or maintain the JRE.) The DMZ Gateway Server component is never executed directly, but rather controlled and monitored using the DMZ Gateway Server Service component.

DMZ Gateway Server Service

The DMZ Gateway Server Service component is responsible for properly initializing the JRE and launching the DMZ Gateway Server component. It then stays resident and provides watchdog monitoring functionality over the DMZ Gateway Server component. It also provides logging and diagnostic capabilities to facilitate troubleshooting any possible issues that may occur during server startup. (Refer to DMZ Gateway Logging for detailed information.)

DMZ Gateway Administration Interface

The DMZ Gateway Administration Interface is a Java-based thick client that provides graphical administration capabilities for the DMZ Gateway Server. The interface communicates with the DMZ Gateway Server via a local-only TCP/IP administration port.

The administration capabilities include:

- Creating and Configuring Profiles
- Viewing Statistics
- Controlling the Server Service/Daemon

DMZ Gateway System Files

The following file names can be observed when running DMZ Gateway:

On Windows Systems:

- In the Windows Services dialog box:
  - DMZ Gateway Server is the DMZ Gateway service.
- In the Task Manager:
  - DMZGatewayServerService.exe launches and monitors the DMZ Gateway Server.
  - DMZGatewayServer.exe is the DMZ Gateway Server.
DMZ Gateway Headless Administration

Configuration and administration of the DMZ Gateway is typically performed using the DMZ Gateway administration interface. This interface runs local to the DMZ Gateway Server and uses a local-only TCP/IP connection to configure the DMZ Gateway Server and to obtain status and statistical information. Administrators of headless systems have the following options for configuring and monitoring the DMZ Gateway:

- Use a remote X11 server to display the administration interface
- Manually configure and monitor the DMZ Gateway Server through the file system

X11 Server Method

While the exact steps required to display the administration interface remotely may differ from system to system, the following steps are typical:

1. Ensure the X11 Server is running on the host system on which the user interface will be displayed.
2. Allow the DMZ Gateway computer access to the X11 Server using the xhost command. For example, issuing the following command in a terminal window on the host system will allow access to all incoming IP addresses:
   
   xhost +

3. Log in to the DMZ Gateway computer as a user with the appropriate permissions to run the DMZ Gateway administration interface.
4. Export the display to the host X11 server by issuing the following command in a terminal window:
   
   EXPORT DISPLAY=<Host IP>:0.0

5. Execute the DMZ Gateway Administration Interface script in a terminal window:
   
   <Installation Directory>/bin/DMZGatewayAdmin
   
   For example:
   
   /opt/dmzgateway/bin/DMZGatewayAdmin
Note that some Unix-based installations come preconfigured in a pure headless fashion and may lack the necessary X11 libraries required to display the administration interface remotely. Please consult your operating system documentation for information on installing the necessary libraries.

**Manual Configuration Method**

The DMZ Gateway Server may be configured by manually editing the DMZ Gateway Configuration file `gwconfig.xml`. For details on the configuration file, refer to [DMZ Gateway Server Configuration File Reference](#).

It is highly recommended that the configuration be edited while the DMZ Gateway Server is not running; changes made to the configuration file will not take effect until the DMZ Gateway Server is restarted.

**DMZ Gateway Logging**

All logging functionality in DMZ Gateway comes preconfigured with the optimal settings. The information below is provided to help you understand what is in the logs. When necessary, modifying the configuration for the logging functionality should only be performed with the aid of Globalscape Customer Support.

The following logs are created and populated during the operation of DMZ Gateway:

- **DMZ Gateway Communications Activity Log** ([DMZActivity.log](#))
- **DMZ Gateway Server Diagnostics Log** ([DMZGatewayServer.log](#))
- **DMZ Gateway Server Service Diagnostics Log** ([DMZGatewayServerService.log](#))
- **DMZ Gateway Statistics Log** ([DMZStatistics.log](#))
- **DMZ Gateway Server Event Viewer** (Windows Operating Systems Only)
- **DMZ Gateway Server Syslog** (Solaris/Linux-based Operating Systems Only)

**DMZ Gateway Communications Activity Logging**

The DMZ Gateway communications activity logging records messages relating to communications to a W3C Extended Log File-formatted file. By default, this log file is created as `<installation directory>\logs\DMZActivity.log`. The format of the log file consists of a header at the beginning of the file and subsequent lines for each communications message generated by the DMZ Gateway Server. (Not all fields will be populated for every message. More information on the W3C Extended Log File format is available on the W3C Web site at [http://www.w3.org/TR/WD-logfile.html](http://www.w3.org/TR/WD-logfile.html).)

*The examples below are for illustration only and do not necessarily reflect your version or installation of DMZ Gateway.*

The header is of the format:

```
#Software: DMZ Gateway Server Version: 3.0.0 build 4
#Version: 3.0
#Date: 2009-09-28 07:31:48
```
#Fields: time status rs-ip rs-comment s-ip s-comment c-ip c-comment

where:

- **Software** – Identifies the application that generated the log file. In this case, the DMZ Gateway Server. This line will also contain the application version and build number of the DMZ Gateway Server.
- **Version** – The version of the extended log file format used.
- **Date** – The date and time the log file was initially created.
- **Fields** – The field names for the fields included in each log message. The fields are defined as:
  - **time** – The date and time the log message was generated
  - **status** – The status of the message where a value of 0 indicates a failure or error and a value of 1 indicates success.
  - **rs-ip** – The remote server IP Address and Port number. This represents the peer server connected to the Peer Notification Channel. This will typically be the EFT.
  - **rs-comment** – Textual status message related to the remote server.
  - **s-ip** – The server IP Address and port. This represents the DMZ Gateway Server.
  - **s-comment** – Textual status message related to the DMZ Gateway Server.
  - **c-ip** – The client IP Address and port. This represents the FTP client connection.
  - **c-comment** – Textual status message related to the client.

The verbosity of messages written to the communications activity log is configurable via the DMZ Gateway administration interface. By default, verbose logging is not enabled. When set to false, only basic communications initialization and de-initialization messages are logged to the activity log. This includes messages concerning Peer Notification Channel listener startups and stops. When verbose logging is enabled, additional communications messages concerning client connections are logged.

Essentially, messages that may occur throughout the course of operating the DMZ Gateway Server are governed by the “Verbose Activity Logging” setting whereas messages that only occur during initial startup and shutdown are always logged. The DMZ Gateway Server appends the log during each run of the DMZ Gateway Server.

The log file will automatically archive itself when reaching 10 MB in size and maintains the last 10 log files in the form `DMZActivity.<X>` where X is a number from 1 to 10, with 1 being the most recently archived log file and 10 being the oldest.
DMZ Gateway Server Diagnostics Logging

The DMZ Gateway Server diagnostics logging functionality provides diagnostic-level messages for the operation of the DMZ Gateway Server. This diagnostic information may be used to identify errors, warnings, and other information of interest that occur during the operation of the DMZ Gateway Server.

By default this functionality logs to the file <installation directory>\logs\DMZGatewayServer.log. The DMZ Gateway Server appends the log during each run of the DMZ Gateway administration interface. The log file automatically archives itself when reaching 10 MB in size and maintains the last 10 log files in the form DMZGatewayAdmin.<X> where X is a number from 1 to 10, with 1 being the most recently archived log file and 10 being the oldest.

DMZ Gateway Server Service Diagnostics Logging

This logging records diagnostic information generated by the DMZ Gateway Server service executable. The diagnostic information may be used to identify errors or warnings that occur during startup of the DMZ Gateway Server. By default, this functionality logs to the following file:

<installation directory>\logs\DMZGatewayServerService.log.

The DMZ Gateway Server appends the log during each run of the DMZ Gateway Server. The log file automatically archives itself when it reaches 10 MB in size and maintains the last 10 log files in the form DMZGatewayServerService.log.<X> where X is a number from 1 to 10, with 1 being the most recently archived log file and 10 being the oldest.

DMZ Gateway Statistics Logging

Statistics logging is disabled by default, because statistics are typically viewed through the DMZ Gateway administration interface. When enabled, this functionality records various statistical data in CSV format to the log file <installation directory>\logs\DMZStatistics.log. A header row is generated at the beginning of each file and then data rows are periodically added for each Profile/Peer Server connection.

The statistical data includes the following fields:

- Timestamp – the date and time the row was generated
- Profile – the Profile to which the row of statistical data pertains
- Server – the Peer Server (e.g. EFT) to which the row of statistical data pertains
- Client Received (B) – the total number of bytes received from clients for the specified Profile/Server.
- Client Sent (B) – the total number of bytes sent to clients for the specified Profile/Server.
- Server Received (B) – the total number of bytes received from the Server for the specified Profile/Server.
- Server Sent (B) – the total number of bytes sent to the Server for the specified Profile/Server.
• Client Receive Rate (Bps) – the number of bytes per second received from clients for the specified Profile/Server.

• Client Send Rate (Bps) – the number of bytes per second sent to clients for the specified Profile/Server.

• Server Receive Rate (Bps) – the number of bytes per second received from the Server for the specified Profile/Server.

• Server Send Rate (Bps) – the number of bytes per second sent to the Server for the specified Profile/Server.

• Connections Accepted – the total number of connections allowed for the specified Profile/Server.

• Connections Refused – the total number of connections refused for the specified Profile/Server.

The log is appended during each run of the DMZ Gateway service. The log file automatically archives itself when reaching 10 MB in size and maintains the last 10 log files in the form DMZGatewayServerService.log.<X> where X is a number from 1 to 10, with 1 being the most recently archived log file and 10 being the oldest.

**DMZ Gateway Server Event Viewer (Windows Operating Systems Only)**

On Windows operating systems, DMZ Gateway records significant events to the Windows Event Log. Events originating from the DMZ Gateway are recorded in the Application Event Log and by default include the following types of events:

• DMZ Gateway Service start
• DMZ Gateway Service stop
• DMZ Gateway Service restart
• DMZ Gateway Service startup failures
• All FATAL and ERROR level diagnostic log messages recorded in the DMZ Gateway Server Diagnostics Log

Additionally, the startup and shutdown activities originating from the Windows Service Control Manager are recorded in the System Event Log.
**DMZ Gateway Server Syslog (Solaris/Linux-based Operating Systems Only)**

On Solaris and Linux-based operating systems, DMZ Gateway can record significant events in the local Syslog. By default, messages will be logged with an indent of “DMZ Gateway Server” to the LOG_USER facility and include the LOG_PID option. (Refer to [http://www.kernel.org/doc/man-pages/online/pages/man3/syslog.3.html](http://www.kernel.org/doc/man-pages/online/pages/man3/syslog.3.html) for information on the syslog functionality or type “man syslog” in a terminal window.)

On Solaris systems, it may be necessary to configure the syslog daemon to include logging of the LOG_USER facility. Typically, you can edit the `/etc/syslog.conf` file as root and add a line such as:

```
user.info <tab> /var/admin/message
```

Replace `<tab>` with an actual TAB character. This will instruct the syslog daemon to log LOG_USER facility messages to the `/var/admin/message` log file. After saving your changes, you will need to restart the syslog daemon as root with a command such as:

```
svcadm restart system-log
```

**DMZ Gateway Administration Interface Logging**

The following log files are created and populated during the operation of the DMZ Gateway administration interface:

- **DMZ Gateway Admin Diagnostics Logging**
- **DMZ Gateway Admin Launcher Diagnostics Logging**

**DMZ Gateway Administration Diagnostics Logging**

The DMZ Gateway administration diagnostics logging provides diagnostic-level messages for the operation of the DMZ Gateway administration interface. This diagnostic information may be used to identify errors or warnings that occur during the operation of the administration interface.

By default this functionality records to the file:

```
<installation directory>/logs/DMZGatewayAdmin.log
```

The log is appended during each run of the DMZ Gateway administration interface. The log file automatically archives itself when reaching 10 MB in size and maintains the last 10 log files in the form `DMZGatewayAdmin.<X>` where X is a number from 1 to 10, with 1 being the most recently archived log file and 10 being the oldest.
DMZ Gateway Admin Launcher Diagnostics Logging

This logging records diagnostic information generated by the DMZ Gateway Admin Launcher executable, `<installation directory>\bin\DMZGatewayAdminLauncher.exe`. This executable is responsible for starting the Java Virtual Machine and launching the DMZ Gateway administration interface. The diagnostic information may be used to identify errors or warnings that occur during startup of the administration application. By default this functionality logs to the file `<installation directory>\logs\DMZGatewayAdminLauncher.log`. This file is overwritten during every execution of the utility.

DMZ Gateway Server Configuration File (gwconfig.xml) Reference

The DMZ Gateway Server configuration file, `gwconfig.xml`, contains the main configuration settings governing communications through the DMZ Gateway Server.

The configuration file is in XML format and its contents are verified against a document type definition (DTD) file `gwconfig.dtd`.

Typically, the configuration items specified in `gwconfig.xml` will be edited via the DMZ Gateway administration interface. However, it is possible to edit the configuration settings using a text editor. Additionally, some advanced configuration items are not available via the DMZ Gateway administration interface and thus will require manual editing to configure.

Changes made to the configuration via manual editing will not take effect until the DMZ Gateway Server is restarted. Thus, the following steps should be followed:

1. Stop the DMZ Gateway Server service/daemon.
2. Edit the `gwconfig.xml` file using a text editor.
3. Save changes to the file.
4. Start the DMZ Gateway Server service/daemon.
5. Verify the DMZ Gateway Server has started and verify that no ERROR or FATAL messages are present in the `DMZGatewayServer.log` diagnostics log file.

Configuration Validation

During startup, the DMZ Gateway Server will load the configuration file and validate its structure against the definition in the DTD file. It will also validate the various data constraints governing each element. If the configuration file format is invalid or the configuration violates any constraints, the DMZ Gateway Server will log an appropriate error message in the diagnostics log `DMZGatewayServer.log` and shut down.
Configuration Elements

Please refer to the DTD file for the valid structure of the configuration file. The following describes the configuration elements available in the gwconfig.xml file.

**ConfigurationVersion**

- The internal version number used to track the configuration file format. *Do not edit.*

**AdminPort**

- The DMZ Gateway administration interface communicates with the DMZ Gateway Server via a local-only TCP/IP communications port to conduct administrative tasks. This configuration item specifies the port to use for this communication path. This setting is not configurable via the user interface and must be edited manually.

  **Valid values:** 0 to 65525.

  Setting the port to 0 instructs the operating system to randomly select an available port from its ephemeral port range.

  Setting the port to 1 through 65535 specifies an exact port. Care should be taken to ensure the specified port is not in use on the system.

  **Default value:** 0

**AdminPortEnabled**

- The DMZ Gateway administration interface communicates with the DMZ Gateway Server via a local-only TCP/IP communications port to conduct administrative tasks. This configuration item allows the user to disable this communication path. Note that disabling the administration port will prevent use of the DMZ Gateway Administration Interface. The DMZ Gateway Server inherently only allows local connections via the administration port. This setting provides an additional level of security by allowing the operator to disable the administration port altogether once initial configuration has been completed. This setting is not configurable via the user interface and must be edited manually.

  **Valid values:**

  true - enable the administration port.

  false – disable the administration port.

  **Default value:** true

**VerboseLoggingEnabled**

- Enables or disables verbose log messages in the DMZ Gateway Server communications activity log file, DMZActivity.log. This setting is configurable via the user interface.

  **Valid values:**

  true - enable verbose log output
false – disable verbose log output

**Default value:** false

**GlobalPNCKeepalivePeriod**

- When a Peer Server application, such as the EFT, is connected to the DMZ Gateway Server via a Peer Notification Channel, keepalive functionality is used to verify that the communications channel is valid and alive. The keepalive functionality verifies the validity of the channel by periodically sending a message to the peer server and verifying that it receives a reply. This setting governs how often this check is performed for all Profiles. This setting is not configurable via the user interface and must be edited manually.

**Valid values:** 1 to 2^63 – 1, in milliseconds

**Default value:** 30000 (30 seconds)

**StatisticsLoggingEnabled**

- The DMZ Gateway Server is capable of periodically logging statistical information to a statistics log file. This setting enables this logging functionality. This setting is not configurable via the user interface and must be edited manually.

**Valid values:**

true - enable statistics logging
false – disable statistics logging

**Default value:** false

**StatisticsLoggingPeriod**

- This setting governs how often the current set of statistics within the DMZ Gateway Server is recorded in the statistics log file. This setting is not configurable via the user interface and must be edited manually.

**Valid values:** 1 to 2^63 – 1, in milliseconds

**Default value:** 300,000 (5 minutes)

**Profiles**

- This element encloses 0 to 15 Profile elements. If no Profiles are specified in the configuration file, the DMZ Gateway Server will automatically create a default Profile during startup. If more than 15 Profiles are defined, the DMZ Gateway Server will log the error during startup and subsequently shut down.
Profile

- This enclosing element contains the configuration items defining a Profile. Profiles are configurable via the administration interface.

ProfileName

- This is the name of the enclosing Profile. The name must be unique among all defined profiles. If the name is not unique, the DMZ Gateway Server will log the error during startup and subsequently shut down. Profile Names are configurable via the administration interface.

  Valid values: From 1 to 260 alphanumeric characters.

  Default value: Profile

ServerIP

- This the IP Address of a local network adapter on which to listen for connections from peer servers on a peer notification channel. Server Listener IPs are configurable via the administration interface.

  Valid values: All or a specific IP address. When "All" is specified, the DMZ Gateway Server will listen on all IP address/port combinations on the local computer that are not already in use.

  Default value: All

ServerPort

- This is the port to use with the IP address(es) specified in the ServerIP element to fully define the IP Address:Port combination on which to listen for connections from peer servers. Server listener ports are configurable via the administration interface.

  Valid values: 0 to 65535. When set to 0 the operating system will randomly select an available port from its ephemeral port range

  Default value: 44500

ClientIP

- This the IP address of a local network adapter on which to listen for connections from clients. Client Listener IPs are configurable via the administration interface.

  Valid values: All or a specific IP address. When "All" is specified, the DMZ Gateway Server will listen on all IP address/port combinations on the local computer that are not already in use.

  Default value: All

PNCKeepalivePeriod

- This element allows optional overriding of the GlobalPNCKeepalivePeriod on a per-Profile basis. This setting is not configurable via the user interface and must be edited manually.

  Valid values: 1 to 2^63 – 1, in milliseconds

  Default value: 30000 (30 seconds)
**NetworkAccessPolicy**

- This enclosing element contains the configuration settings for the IP access policy used to validate connections to the Peer Notification Channels of the enclosing Profile. The Network Access Policies for each Profile are configurable via the administration interface.

**DefaultAccessPolicy**

- This is the policy to use by default when validating connections to the Peer Notification Channels of the enclosing Profile. The Default Access Policy for each Profile is configurable via the administration interface.

  **Valid values:**
  
  Grant – by default all connections will be granted access.

  Deny – by default all connections will be denied access.

  **Default value:** Grant

**GrantPolicyExceptions**

- This element encloses 0 or more Exception elements that act as exceptions to the Grant All policy. Thus, they define what will be denied access. A maximum of 100 Exception elements may be defined. If more than 100 are defined, the DMZ Gateway Server will log the error during startup and subsequently shut down. The Grant Policy Exceptions for each Profile are configurable via the administration user interface.

**DenyPolicyExceptions**

- This element encloses 0 or more Exception elements that act as exceptions to the Deny All policy. Thus, they define what will be granted access. A maximum of 100 Exception elements may be defined. If more than 100 are defined, the DMZ Gateway Server will log the error during startup and subsequently shut down. The Deny Policy Exceptions for each Profile are configurable via the administration user interface.

**Exception**

This element defines an exception to the enclosing Policy type. Exceptions are implemented as IP address masks that allow definition of masks that may be used to match the IP Address of a connecting peer server. The exceptions are configurable via the administration interface.

**Valid values:** IP Address Masks match against IPv4 or IPv6 IP addresses
File Location

For new installs, the configuration file is created the first time the DMZ Gateway Server is started. When the configuration file is created, the corresponding DTD file is also created. By default, the configuration and DTD files are created in the DMZ Gateway installation directory. However, to facilitate sharing of configuration data in high availability clustered installs, an alternate shared data location may be specified.

Shared Configuration Location

An alternate shared data location may be specified either during the installation process or by subsequently editing the `DMZGatewayServerService.conf` file.

To specify the shared data location:

1. Stop the DMZ Gateway Server Service/Daemon.
2. Edit the `<Installation Directory>\con\DMZGatewayServerService.conf` file using your preferred text editor.
3. Locate the following line in the file:
   ```
   set.DMZ_SHARED_CONFIG_DIRECTORY=""
   ```
4. Edit the line and enter the shared data location within the quotes, for example:
   - On Windows: `set.DMZ_SHARED_CONFIG_DIRECTORY="\jupiter\DataShare\DMZGateway"
   - On Solaris/Linux: `set.DMZ_SHARED_CONFIG_DIRECTORY="/export/share/dmzgateway"
5. Save the changes to the file.
6. If you want to reuse the settings in the existing `gwconfig.xml` configuration file, move the file to the new location.
7. Start the DMZ Gateway Server Service/Daemon.

Please ensure that the operating permissions governing the DMZ Gateway Server service/daemon are set such that the process is able to access the specified shared configuration directory.

Note that the DMZ Gateway Server will automatically (re)generate the `gwconfig.dtd` DTD file in the specified shared data location. Additionally, for convenience, the file will also be generated in the installation directory.

DMZ Gateway Server Unix/Solaris Daemon

On Solaris and Linux-based system, the DMZ Gateway Server is started and controlled using the system daemon script `<Installation Directory>/bin/dmzgatewayd`. When necessary, this script will call the Java Service Wrapper utility `<Installation Directory>/bin/DMZGatewayServerService` to start and stop the `DMZGatewayServer` Java executable.
Per convention, if the user opted to register the service with the operating system during installation, a symbolic link `/etc/init.d/dmzgatewayd` will have been created. This symbolic link points to the `<Installation Directory>/bin/dmzgatewayd` script. Additionally, the appropriate symbolic links will have been created in the `/etc/rc.d` directories so that the DMZ Gateway Server will be started and stopped appropriately during system startup and shutdown.

You can control the system daemon by executing either `/etc/init.d/dmzgatewayd` or `<Installation Directory>/bin/dmzgatewayd`. The script accepts a set of command line options. Running the script without any command line options will display the set of available options, which are itemized below:

- **console** – Runs the DMZ Gateway Server as a console program as opposed to a system daemon.
- **start** – Starts the DMZ Gateway Server as a daemon process
- **stop** – Stops the DMZ Gateway Server daemon process, if running.
- **restart** – Stops the DMZ Gateway Server daemon process, if running, and then starts it.
- **condrestart** – Restarts the DMZ Gateway Server daemon process if it is currently running.
- **status** – Indicates if the DMZ Gateway Server daemon process is currently running or not.
- **dump** – Instructs the Java Virtual Machine to log the state of all active threads to the log.

**DMZ Gateway Status**

The top pane of the DMZ Gateway interface displays the DMZ Gateway service status and the selected profile’s status. The pane displays:

- When DMZ Gateway service is stopped.
- When DMZ Gateway service is running but no Site is connected to the selected profile.
- When DMZ Gateway service is running and there is a Site connected to the profile and a port is assigned.
- When DMZ Gateway service is running and there is a Site connected to the profile, but no port is assigned.

![DMZ Gateway Enterprise](image)

When the **All Profiles** node is selected, as shown below, the **Server Status** area displays the size of items transferring through DMZ Gateway. (Because **All Profiles** is selected, no status appears in the Selected profile status area.)
Server statistics include:

- Accepted Client Connections - Count of client connections accepted through the DMZ Gateway during the current run of the DMZ Gateway
- Rejected Client Connections - Count of client connections rejected through the DMZ Gateway during the current run of the DMZ Gateway
- Connections Closed - Count of connections closed during the current run of the DMZ Gateway
- Active Client Connections - Count of the currently active client connections
- Client Bytes Read - Number of bytes received from Clients
- Client Bytes Written - Number of bytes sent to Clients
- EFT Server Bytes Read - Number of bytes received from Servers
- EFT Server Bytes Written - Number of bytes sent to Servers
- Client Bytes Read/s - Transmission speed when receiving from Clients in bytes per second (B/s)
- Client Bytes Written/s - Transmission speed when sending to Clients in bytes per second (B/s)
- EFT Server Bytes Read/s - Transmission speed when receiving from Servers in bytes per second (B/s)
- EFT Server Bytes Written/s - Transmission speed when sending to Servers in bytes per second (B/s)
When the All Profiles node is selected, a check box appears at the bottom of the right pane that allow you to enable or disable debug logging.

**Error Codes**

The following error codes can appear in logs, error messages, and the Windows Event Viewer.

**To start Event Viewer by using the Windows interface**

1. Click the Start button.
2. Click Control Panel.
3. Click System and Maintenance.
4. Click Administrative Tools.
5. Double-click Event Viewer.

**To start Event Viewer by using a command line**

1. Open a command prompt. To open a command prompt, click Start, click All Programs, click Accessories and then click Command Prompt.
2. Type:
   ```
eventvwr
   ```

**Editing a Profile**

When you create a new Profile, you define the listening IP address for remote connecting clients, the listening IP address and port for the server inside your network, and any IP addresses exceptions. After the Profile is created, you can edit the Profile’s configuration as necessary. You can also rename or delete the Profile.

When you make a change to a Profile, before you click Apply, an asterisk appears in the tree next to the Profile that you are editing. You must define a unique IP address/port combination for each Profile.

**To edit a Profile**

1. In the Navigation pane, click the Profile that you want to edit.
2. In the Configuration pane, click the General tab.
3. Specify the Listening IP for incoming Clients box and the Listening IP for Server. Refer to Specifying the Listening IP Addresses for detailed information.
4. In the Port box, provide the port number over which connections are allowed.
5. In the Configuration pane, click the Access tab.
6. Specify the IP addresses or IP mask of servers that are allowed or denied access.

7. In the toolbar, click Apply Changes. If the IP address and port are not unique, an error message appears; otherwise, the DMZ Gateway will allow the server to connect.

If you have made multiple edits, you can revert to the last-saved state by clicking Revert Changes (undo) before clicking Apply Changes. However, once you click Apply Changes, you cannot go back.

Internal Domain Settings

The Internal Domain Settings dialog box on the DMZ Gateway tab, is used to configure separate external and internal domain access. See Specifying External and Internal Domains and Allow LDAP Authentication through DMZ for more information about how to do that. Below are some diagrams to visually describe how the two check boxes, Allow LDAP authentication to EFT through DMZ Gateway and Make LDAP authentication exclusive for internal connections, interact to determine external and internal user access.

1. When neither box is selected, EFT and DMZ Gateway are in a "split domain" configuration:
   - LDAP users are only allowed to log in through the internal (EFT) URL; they cannot use the external (DMZ Gateway) URL.
   - Globalscape authentication users can log in through the external (DMZ Gateway) URL or the internal (EFT) URL.
2. When the **Allow LDAP authentication to EFT through DMZ Gateway** check box is selected, (but **not** the **Make LDAP authentication exclusive for internal connections** check box):
   -Globalscape authentication users and LDAP users can log in using the internal (EFT) URL OR external (DMZ Gateway) URL. This configuration allows remote users to access EFT through DMZ Gateway.

3. When the **Make LDAP authentication exclusive for internal connections** check box is selected (but **not** the **Allow LDAP authentication to EFT through DMZ Gateway** check box):
   - LDAP users can only log in using the internal (EFT) URL; they cannot use the external (DMZ Gateway) URL.
   -Globalscape authentication users can log in using only the external (DMZ Gateway) URL; they cannot use the internal (EFT) URL.
4. When both the **Allow LDAP authentication to EFT through DMZ Gateway** check box and the **Make LDAP authentication exclusive for internal connections** check box are selected:

- Only LDAP users can log in using the internal (EFT) or external (DMZ Gateway) URL
- Globalscape authentication users can only log in using the external (DMZ Gateway) URL; they cannot log in using the internal (EFT) URL.

---

**Renaming a Profile**

The Profile name appears in statistics, logs, messages, and reports. You can change the name in the DMZ Gateway interface.

**To change the name of a Profile**

1. Click the Profile in the tree, then do one of the following:
   - Click the Profile name again.
   - Right-click the Profile name, then click **Rename Profile**.
• On the toolbar, click **Rename Profile**.

• On the main menu, click **Profile > Rename**.

The name in the tree becomes editable.

2. Type a new name for the tree, then press ENTER.

**Routing AS2 Traffic through DMZ Gateway**

*Using the DMZ Gateway as proxy is available only in EFT Enterprise.*

You can configure Event Rules to cause AS2 traffic to route through the DMZ Gateway using the **AS2 Send file to host** Action. You can use the **AS2 Send File to host** Action in the Folder Monitor, Timer, and all file-based Events.

**To route AS2 traffic through DMZ Gateway**

1. Create a new Event Rule, such as a File Uploaded event. (If necessary, refer to "Creating Event Rules" in the EFT Server documentation.)

2. Add the **AS2 Send file to host** Action to the Rule, then click the file or host link. The **AS2 Send File** dialog box appears.

3. In the **AS2 Send File** dialog box, specify trading partner profile to use or define the trading partner options.

4. Add the **Copy/Move File to Host** Action to the Rule.

5. In the **Rule** pane, click one of the undefined parameters (e.g., '%FS.PATH%'). The **Offload Action Wizard** appears.

6. Follow the instructions in **Using DMZ Gateway as an Outbound Proxy** to define the Rule.
Specifying the Listening IP Addresses

For each DMZ Gateway Profile, you specify 2 IP addresses:

1. One address is used by client programs to connect. This is typically an external-facing address. When a Site configured at a peer server connects to the DMZ Gateway over the PNC, the DMZ Gateway reads the list of client ports configured in the Site. These ports are then combined with the client IP Address and it is on these client IP address/Site port combinations that the DMZ Gateway will listen for client connections.

2. The other address specifies the IP address on which to listen for connections from peer servers. The communications established using this address is known as the Peer Notification Channel or PNC. Typically, this IP Address will be an internal-facing address. This address is combined with the configured port value and it is on this IP Address/port combination that the DMZ Gateway will listen for connections from peer servers.

If you are using the Accelerate module in EFT, you should also specify the Listening IP for Acceleration. Each address is configured by selecting the IP address to use from a drop-down list. The list of IP addresses includes all IPv4 and IPv6 addresses present on the computer. Additionally, the list includes an All Available setting for both IPv4 and IPv6. (IPv6 connections to DMZ Gateway are not supported on Windows Server 2003.)
• In the **Listening IP for incoming Clients** box, click the down arrow to select one or more IP addresses for incoming clients. (Only the IP addresses defined on this computer appear in this box.) You can specify:
  
  o **All Available (IPv4)**—Listen for client connections on all IPv4 addresses.
  
  o **All Available (IPv6)**—Listen for client connections on all IPv6 addresses.
  
  o **All Available (IPv4 and IPv6)**—Listen for client connections on all IPv4 and IPv6 addresses.
  
  o **A specific IP address**—Listen for client connections on all on a specific IP address.

• In the **Listening IP for Server** box, click the down arrow to select one or more listening IP addresses for the server. (Only the IP addresses defined on this computer appear in this box.) **All Available** means that DMZ Gateway will listen on the IP address/port combination ONLY IF that IP address/port combination is not already being used by another Profile. Profiles configured with an explicit IP address have precedence over Profiles configured with **All Available**. You can specify:
  
  o **All Available (IPv4)**—Listen for server connections on all IPv4 addresses.
  
  o **All Available (IPv6)**—Listen for server connections on all IPv6 addresses.
  
  o **All Available (IPv4 and IPv6)**—Listen for server connections on all IPv4 and IPv6 addresses.
  
  o **A specific IP address**—Listen for server connections on all on a specific IP address.

**IMPORTANT:**

**All Available** means that DMZ Gateway will listen on the IP address/port combination ONLY IF that IP address/port combination is not already being used by another Profile. Profiles configured with an explicit IP address have precedence over Profiles configured with **All Available**.
What Does This Mean for the Peer Server Listeners?

Suppose you have three IP addresses on the computer: IP 1, IP 2, and IP 3, and you have two Profiles: Profile 1 and Profile 2.

- Both Profiles are configured to use the same Peer Server Listener Port 54321.
- Profile 1 is set to use All Available.
- Profile 2 is set to use IP 2.

Profile 1 will listen on **IP 1:54321** and **IP 3:54321**, and Profile 2 will listen on **IP 2:54321**.

Now, suppose you delete Profile 2, making IP 2:54321 available. The DMZ Gateway will detect this and update the communications listeners so that Profile 1 will now listen on **IP 1:54321**, **IP 2:54321**, and **IP 3:54321**.

What Does This Mean for the Client Listeners?

Suppose you have three IP addresses on the computer: IP 1, IP 2, and IP 3, and you have two Profiles: Profile 1 and Profile 2. Profile 1 is set to use All Available and Profile 2 is set to use IP 2.

Now suppose you have two Sites configured on EFT. Both Sites are configured to connect to the DMZ Gateway and use FTP port 21. Site 1 is set to connect to Profile 1, and Site 2 is set to connect to Profile 2.

Once both Sites are connected, the DMZ Gateway will establish client listeners for Site 1 on **IP 1:21** and **IP 3:21** (because Site 1 used Profile 1, which uses all available IP/port combinations not currently in use). For Site 2 the DMZ Gateway will establish a client listener on **IP 2:21**.

If Site 2 should disconnect for some reason (perhaps it was deleted), **IP 2:21** is now considered available. The DMZ Gateway will detect this and update the communications listeners so that Profile 1 will listen for client connections on **IP 1:21**, **IP 2:21**, and **IP 3:21**.

Specify Whether DNS Lookup is Performed on EFT or DMZ Gateway

By default, when using DMZ Gateway as a proxy, the DNS lookup is handled on EFT. If you have a secured environment in which no DNS lookup is performed in the DMZ of the network, or if you have a split DNS between EFT and DMZ Gateway, you can add a registry setting use DMZ Gateway for DNS. 1 = use DMZ Gateway for DNS; 0 or no registry key = use EFT for DNS lookup.

To configure the registry setting

1. In the registry, navigate to

   ```plaintext
   HKEY_LOCAL_MACHINE\Software\Wow6432Node\GlobalSCAPE Inc.\EFT Server 7.3\[1]
   ```

2. Right-click the node, then click **New > DWORD value**.

3. Value name:

   ```plaintext
   DMZResolvesDNSNames
   ```

4. Value data: 1 (Default Value: 0, not enabled)

---

[1]: HKEY_LOCAL_MACHINE\Software\Wow6432Node\GlobalSCAPE Inc.\EFT Server 7.3\[1]
5. Close the registry and restart the Site.

Starting and Stopping the DMZ Gateway Server Service

Typically, the DMZ Gateway server service is configured to start automatically when the computer is started. When the DMZ Gateway administration interface is launched, it determines whether the DMZ Gateway server service is running. If the DMZ Gateway server service is not running, a prompt appears asking if you want to start the DMZ Gateway service.

On Windows systems:

When you install DMZ Gateway, the service is configured to start automatically. You can start and stop the service in the Windows Services dialog box and in the DMZ Gateway Administration Interface.

On non-Windows systems:

The installation script includes registering and starting the DMZ Gateway server daemon (configuring it to auto-start on system start and auto-stop on system stop). Alternatively, you can start and stop the server manually using the following commands:

<InstallDir>/bin/dmzgatewayd start
<InstallDir>/bin/dmzgatewayd stop

In the DMZ Gateway administration interface:

In the DMZ Gateway administration interface, you can start and stop the service from the Server menu or using the toolbar controls. The status of the DMZ Gateway server service appears in the status bar at the bottom of the interface. (e.g., “DMZ Gateway is running.”) You can start, pause, restart, or stop the DMZ Gateway service on the DMZ Gateway main menu or toolbar.

To start the DMZ Gateway

• On the DMZ Gateway main menu, click Server > Start or click Start on the toolbar.

To restart the DMZ Gateway

• On the DMZ Gateway main menu, click Server > Restart or click Restart on the toolbar.

To stop the DMZ Gateway

• On the DMZ Gateway main menu, click Server > Stop or click Stop on the toolbar.

DMZ Gateway Server PID Files

When the DMZ Gateway Server Service starts it will create the PID file <Installation Directory>\DMZGatewayServerService.pid. This file contains the process ID for the DMZ Gateway Server Service.

When the DMZ Gateway Server is started, the PID file <Installation Directory>\DMZGatewayServer.pid is created. This file contains the process ID for the DMZ Gateway Server.
DMZ Gateway Server Status Files

During the course of operation, the DMZ Gateway Server Service will create and update the status file <Installation Directory>\DMZGatewayServerService.status. This file will contain the current status of the DMZ Gateway Server Service. The possible contents are described at http://wrapper.tanukisoftware.org/doc/english/prop-statusfile.html.

During the course of operation the DMZ Gateway Server Service will create and update the status file <Installation Directory>\DMZGatewayServer.status. This file will contain the current status of the DMZ Gateway Server. The possible contents are described at http://wrapper.tanukisoftware.org/doc/english/prop-java-statusfile.html.

DMZ Gateway Server Monitoring

After starting the DMZ Gateway Server, the DMZ Gateway Server Service will stay resident and monitor the Server. If the Server crashes, the Service will wait 5 seconds and attempt to restart the Server.

Testing the Configuration

After you have installed DMZ Gateway, created and configured a Profile, and enabled DMZ Gateway in EFT, you can test your configuration by connecting to the server via DMZ Gateway and transferring a few files.

To test your configuration

Suppose your server is at IP address 192.168.174.176 and DMZ Gateway is at IP address 192.168.174.142, and you have configured DMZ Gateway in the server to allow connections over the HTTPS port 443.

1. Open a browser and in the address bar type https://192.168.174.142 (the IP address of DMZ Gateway), then press ENTER.
2. You should be prompted to log in. Type the login credentials from a user defined on the server to which you want to connect.
3. Transfer a few files.
4. On the Status tab, you should see the numbers increase in the Client Bytes Read, Client Bytes Written, Server Bytes Read, and Server Bytes Written columns. Click Refresh, if necessary. (Note that if you connect to the server’s IP address to transfer files, you are not going through the DMZ Gateway and, therefore, will not see any statistics change.)
   - In the folder for the account that you used to log in (e.g., C:\inetpub\EFTRoot\GSSite\Usr\<username>), you should see the files that you transferred.
5. If you are not able to connect, refer to Troubleshooting DMZ Gateway Communication.
Troubleshooting DMZ Gateway Communication

Various configurations can prevent the server and DMZ Gateway from communicating. For example, if the DMZ Gateway computer’s firewall is blocking connections, the server will not be able to connect to DMZ Gateway.

If the status icon in DMZ Gateway does not change color to green indicating a successful connection, verify the following:

1. Verify that the services for the server and DMZ Gateway are started.
2. If you make changes in DMZ Gateway, make sure to click **Apply Changes**. If necessary, in the server, stop and then restart the service (and/or the Site in EFT) after making changes.
3. If you made configuration changes in EFT, especially connection settings (protocols allowed, ports, etc.), make sure to stop and then restart the EFT service. Once restarted, make sure EFT is running (listening for new connections) and that DMZ Gateway remains enabled.
4. Verify that the IP address for the server is not blocked in DMZ Gateway’s **IP Access Exception** list. By default, all IP addresses are granted access until you block or allow specific addresses. (Refer to [Controlling Access by IP Address](#) for the procedure for blocking/unblocking IP addresses.)
5. Verify that the **DMZ Gateway settings in the server** have the proper IP address and port and that the allowed protocols and ports have been defined for allowed incoming client connections.
6. Try pinging from the server computer to the DMZ Gateway computer and from the DMZ Gateway computer to the server computer. If you cannot connect, verify that there is no firewall that would block connections.

If a connection between the server and DMZ Gateway is indicated, but clients cannot connect to the server through DMZ Gateway:

Verify that you can connect to the server using a client account from within your network.

If connection is successful, but clients cannot connect through DMZ Gateway, something is not configured properly in the DMZ Gateway settings, either in DMZ Gateway or in the server. Verify that the server and DMZ Gateway are connected (see above) and that, in the server <= -> DMZ Gateway configuration settings, the correct protocols and ports are specified for incoming client connections to the Gateway. These are the ports on which external clients will connect to DMZ Gateway. If no protocol is enabled or the wrong port is defined, clients will not be able to connect.

If connection fails, there is a configuration issue in the server. Review your configuration of user accounts and connection settings.
Using DMZ Gateway as an Outbound Proxy

DMZ Gateway's primary use is as an inbound proxy. Outbound connections that originate from EFT Enterprise will route through normal network mechanisms to reach the destination; however, it is possible to configure EFT's Event Rules using the Copy/Move file to host Action to use DMZ Gateway Enterprise as an outbound proxy.

Viewing Statistics

In the DMZ Gateway administration interface, you can view a variety of statistics. Whether you click All Profiles or a specific Profile, the Status area displays information about Peer Notification Channels and Client Listeners, as well as the size and speed of server and client data being transferred.

Your selections persist across Profiles; that is, if you click the Client Listeners tab in Profile 3, then click Profile 2, the Client Listeners tab is selected in Profile 2 also.

The status “bubbles up” to the All Profiles node. For example, if there is a problem in Profile 1 causing the icon to turn yellow, the All Profiles icon is also yellow.

In the Profile tree:

- A red icon 🟥 indicates that an error exists (e.g. port conflict from external application, IP address no longer exists, etc.).
- A yellow icon 🟢 indicates that the DMZ Gateway service is running, but port conflicts exist between connected sites, when at least two Sites are connected.
- A green icon 🟢 indicates that the DMZ Gateway Service is running and at least one Site is connected.
- A gray icon 🟢 indicates that there are no errors and no Servers are connected.

Peer Notification Channels Tab

The Peer Notification Channels tab of the Status panel displays the IP address, port, number of active sites, channel status, and channel status message for each configured server-side IP address for a selected Profile or All Profiles. If All Profiles is selected, a Profile column displays the name of the applicable Profile. (For more about Peer Notification, refer to Introduction to Globalscape DMZ Gateway.)

The following icons provide an indication of channel status:

- 🟢 Active with connected servers
- 🟢 Active with no connected servers
- 🟢 Warning
- 🟢 Error

The following columns displayed on the tab can be sorted by clicking the column header:

- IP address - IP address on which Peer Notification Channels communicate
- Port - Port on which Peer Notification Channels communicates
- **Active Sites** - Number of Sites connected to DMZ Gateway
- **Status** - Active, Inactive, Warning, Error
- **Message** - More information regarding status (e.g., Listening for connections, Port already in use)

### Client Listeners Tab

The **Client Listeners** tab of the **Status** panel displays the PNC address, server IP address, server name, server type, Site name, listener IP address/port, status, and status message. If **All Profiles** is selected, the **Profile** column displays the name of the applicable Profile.

The following icons provide an indication of status:

- ![Listening](listening.png)
- ![Inactive](inactive.png)
- ![Warning](warning.png)
- ![Error](error.png)

The following columns displayed on the tab can be sorted by clicking the column header:

- **PNC Address** - Server-side IP address on which the server connected to DMZ Gateway
- **Server IP Address** - IP address of the remote server
- **Server Name** - user-assigned name of connected server
- **Server Type** - Type of server, e.g., EFT, EFT Enterprise
- **Site** - User-assigned name of Site
- **Listener IP Address** - Client-side IP address on which clients connect to DMZ Gateway
- **Listener Port** - Port of Listener
- **Status** - Active, Inactive, Error, Warning
- **Message** - More information regarding status (e.g., Listening for incoming connections, Unable to bind to port, Listener creation failure, Closed, Inactive, Listener IP/Port address already assigned)
Statistics Tab

The Statistics tab of the Status panel displays the size and speed of server and client data being transferred. When All Profiles is selected, the aggregated data sizes are displayed, and the Profile column displays the name of the applicable Profile.

The Statistics tab is configured by default to refresh automatically every 15 seconds. You can change the refresh frequency or configure the interface to not refresh automatically. You can also refresh the display manually.

- To change the refresh frequency, in the Refresh Interval box, provide a new interval, in seconds, then click Apply Refresh Interval.
- To prevent the interface from refreshing automatically, clear the Enable automatic refresh check box.
- To refresh the interface manually, click Refresh Now.

The following columns displayed on the tab can be sorted by clicking the column header:

- Server IP Address - IP address of the server
- Client Bytes Read/sec - Number of bytes received from Clients
- Client Bytes Written/sec - Number of bytes sent to Clients
- Server Bytes Read/sec - Number of bytes received from Servers
- Server Bytes Written/sec - Number of bytes sent to Servers
- Accepted Client Connections - Number of successful client connections.
- Rejected Client Connections - Number of client connections attempted that were rejected.

DMZ Gateway Secure PNC

The topics in this section describe how to enable and configure secure PNC in DMZ Gateway and EFT.

Introduction to Secure PNC

EFT administrators might want to administer EFT from a location external to the network by connecting through the DMZ Gateway instead of having to RDP in to the server. The Peer Notification Channel (PNC) between DMZ Gateway and EFT is not, itself, encrypted. Instead, the PNC leverages the encryption provided by the secure protocols (e.g., FTPS, SFTP, HTTPS) in EFT. This inherently encrypts the traffic traversing through the DMZ Gateway and traffic will remain encrypted until it reaches EFT. In this way, the PNC is not susceptible to man-in-the-middle attacks and does not present any real world security risks as long as EFT is using secure protocols.

If you want to further enhance the security of the data passing through DMZ Gateway, you can enable secure PNC settings in DMZ Gateway and EFT. The secure PNC settings will reduce false positives for security scans and reduce the attack vector.
**Remote Administration of EFT**

EFT shares its Site-level manual IP access list and permanent auto-ban IP (not temporary auto-ban) list to DMZ Gateway so that it can block IP addresses before reaching EFT.

Now that remote administration can be routed through DMZ Gateway, we allow EFT to transmit the remote administration manual IP access list to DMZ Gateway for the same purpose. For a client to perform remote administration through DMZ Gateway, its IP must pass both the Site-level and remote administration IP access validation. Note that the remote administration auto-ban feature in EFT is hardcoded to ban IP addresses temporarily, NOT permanently. Therefore, this auto ban list is not communicated to DMZ Gateway and rather it is enforced by EFT itself.

For customers with a new version of EFT supporting the remote administration through DMZ Gateway feature, and with an older DMZ Gateway, they can still do remote administration through DMZ Gateway, but only Site-level manual and Site-level permanent auto-ban IP access lists will be enforced at the DMZ Gateway. Remote administration IP access lists will be enforced only by EFT.

**Notes to consider:**

1. To enable remote administration through DMZ Gateway, you’ll need to enable remote administration in the EFT administration interface at the Server level and select the **Require SSL for remote administration** check box.

2. The Site and remote administration **IP access/ban lists** in EFT are combined at DMZ Gateway. If there is a conflict, e.g., the remote administration block list allows an IP address that is blocked at the Site level, then the IP address will be blocked (least privileges assignment).

3. If EFT automatically bans an IP address temporarily (as result of DoS/Flooding or other trigger), that IP address will **not** be shared with the DMZ Gateway. The administration access will still be blocked, but at EFT, not DMZ Gateway. The administrator can manually add those IP addresses to the permanent ban list, which will propagate to DMZ Gateway.

4. EFT can work with older DMZ Gateway versions (v<3.5) and still allow remote administration; however, when connected to an older DMZ Gateway, any IP address in the administration access/ban list will **not** be shared with the DMZ Gateway, as the older versions do not support receiving the administration IP access/ban list. Again, EFT will still block the connection, but DMZ Gateway will not.

5. If you are remotely connected to EFT via DMZ Gateway and make a change to the EFT<->DMZ Gateway settings, including disconnecting EFT from DMZ Gateway, the active session will not be affected. If/when you attempt to reconnect to EFT via DMZ Gateway, you will experience the effects of any changes.
Configuring Secure PNC

Secure PNC will work using a self-signed certificate created with OpenSSL or one created from EFT. Depending on the certificate used, different configuration steps must be taken, as described below.

There are two ways of authenticating the communication between EFT and DMZ:

- **Non-mutual authentication**
  - EFT will blindly trust the DMZ Gateway certificate and DMZ Gateway will blindly trust the EFT certificate.

- **Mutual authentication**
  - EFT will only trust that single certificate and DMZ Gateway will require EFT to provide a client certificate during the SSL handshake and it must match the DMZ Gateway server’s certificate trust store.

Configuring Secure PNC using a Self-Signed Certificate

To configure Secure PNC using a self-signed certificate

1. Stop the DMZ Gateway Service.
2. On the DMZ Gateway server, open a command prompt and navigate to `C:\Program Files\GlobalSCAPE\DMZ Gateway\bin\jre1.8.0_74\bin\`.
3. Type the following command to create a self-signed certificate:
   ```
   keytool -genkeypair -alias test -keyalg RSA -validity 365 -keystore keystore.jks
   ```
4. Enter a keystore password (e.g., test123!).
5. Follow the prompts for creating the self-signed certificate.
6. Follow the steps for Non-Mutual Authentication between EFT and DMZ or steps for Mutual Authentication between EFT and DMZ, above.

Configuring Secure PNC using an EFT Certificate

This certificate will be used later for Mutual Authentication with the DMZ Gateway server.

The procedure below requires OpenSSL to convert the public and private EFT keys into a .p12 format and Java’s keytool to create a keystore.jks file.

To configure Secure PNC using an EFT-generated certificate

1. Install EFT Server.
2. Launch the EFT administration interface.
3. Create the default Site with SSL enabled.
4. Create a new SSL Certificate, making sure the certificate password is at least 6 characters long. (This certificate will not be associated with any EFT Site; this is used instead of creating a certificate using OpenSSL.)

5. Install OpenSSL (use version 1.0.2 or later).

6. Copy the private and public certificates from Step 4 into the bin directory of OpenSSL (this makes it easier), C:\OpenSSL-Win32\bin\.

7. Using OpenSSL, run the following (update where necessary):


   (Refer to https://www.wowza.com/docs/how-to-import-an-existing-ssl-certificate-and-private-key for information about how to convert the certificate and private key to PKCS 12 (.p12).)

8. If you see a warning related to “can't open config file,” then cancel the entry from Step 7 and run this command instead:

   set OPENSSL_CONF=[path-to-OpenSSL-install-dir]\bin\openssl.cfg (i.e. set OPENSSL_CONF=c:\OpenSSL-Win32\bin\openssl.cfg)

9. When prompted for a passphrase, enter the certificate password you used when this certificate was created in EFT.

10. On the DMZ Gateway server, use Windows Explorer to navigate to the DMZ Gateway installer's /bin/ path, e.g., C:\Program Files\GlobalSCAPE\DMZ Gateway\bin\jre1.8.0_74\bin.

11. Copy the .p12 certificate from Step 7 into the DMZ Gateway installer's /bin/ path in the previous step. (This makes it easier to create the keystore.jks file.)

12. Open Command Prompt to the DMZ Gateway installer's /bin/ path and enter the following command (update where appropriate):


   (where password is the original password set when the private key was created in Step 4)

You have successfully created a keystore.jks file that can be used to use non-mutual authentication between EFT and DMZ, described below.

Non-Mutual Authentication setup

1. For simplicity, you can copy the keystore.jks file that was created above to a path that is easily accessible (e.g., C:\keystore\keystore.jks), because you will have to paste the path in the DMZ Gateway xml configuration file.

2. Open Notepad or another text editor as an administrator.

3. Open the DMZ Gateway configuration file (gwconfig.xml), located in C:\Program Files\GlobalSCAPE\DMZ Gateway.
(If the configuration file does not exist, start or restart the service and the file will be created.)

4. Set the `<SecurePNCEnabled>` value to "true."

5. Set the `<PNCKeyStorePath>` to the path where the `keystore.jks` is located (e.g., `C:\keystore\keystore.jks`)

   **NOTE** You must enter the proper XML format for these values otherwise the service will not start, e.g., `<PNCKeyStorePath>c:\keystore\keystore.jks</PNCKeyStorePath>`

6. Enter the store passphrase; because we imported the certificate into the keystore, this will default to the password created in EFT’s certificate creation.

7. Save the XML file.


9. Start the DMZ Gateway service.

10. Re-open the XML file and verify the passphrase is now encrypted (this will also help confirm DMZ picked up the changes).

   **NOTE** If you are making any changes to the XML file, make sure the DMZ Gateway service has been stopped **prior to** making the changes.

11. To verify EFT detects that DMZ is configured, launch the EFT administration interface.
12. Click the **DMZ Gateway** tab.

13. Enable DMZ Gateway and provide the IP address of the DMZ Gateway, but do not select the Secure TLS/PNC check box.

14. Click **Apply**.

15. Verify that the EFT administration interface receives an error message.

16. Click **OK** on the error message.

17. Select the **Secure (TLS) Peer Notification Channel (PNC)** check box.

18. Click **Apply**.

DMZ Gateway and EFT are now configured with PNC SSL+ non-mutual authentication.
Mutual Authentication Setup

1. Copy the EFT SSL Site certificate (certificate associated with the SSL certificate settings) into the DMZ bin directory, e.g., C:\Program Files\GlobalSCAPE\DMZ Gateway\bin\jre1.8.0_74\bin.

2. Stop the DMZ Gateway Service.

3. To import EFT’s SSL site certificate into the DMZ’s Java truststore, open a command prompt and navigate to C:\Program Files\GlobalSCAPE\DMZ Gateway\bin\jre1.8.0_74\bin.

4. Run the following command:
   ```bash
   keytool -import -alias EftClientCert -file "MySite Certificate.crt" -keystore truststore.jks
   ```

5. When prompted, enter the password of the keystore (not the password of the EFT site’s certificate).

6. When prompted, type yes and press ENTER to trust the certificate.

7. Copy truststore.jks from the C:\Program Files\GlobalSCAPE\DMZ Gateway\bin\jre1.8.0_74\bin and place it in an easily accessible location (e.g., C:\keystore\truststore.jks).

8. Open Notepad (or another text editor) as an administrator.

9. In Notepad, open the DMZ Gateway configuration (XML) file: C:\Program Files\GlobalSCAPE\DMZ Gateway\gwconfig.xml

10. Add the PNCTrustStorePath value, e.g.,
    ```xml
    <PNCTrustStorePath>c:\keystore\truststore.jks</PNCTrustStorePath>
    ```

11. Save and close the XML file.

12. To export the truststore certificate, open a command prompt and navigate to C:\Program Files\GlobalSCAPE\DMZ Gateway\bin\jre1.8.0_74\bin.

13. Run the following command:
    ```bash
    keytool -export -alias test -keystore keystore.jks -rfc -file DMZGatewayCert.cer
    ```

14. If you don’t recall the alias that you used, type the following command:
    ```bash
    keytool -list -v -keystore keystore.jks
    ```
    (This will give you the alias of your keystore)

15. When prompted enter the password of the keystore.

16. Copy the newly created certificate to EFT.

17. Log in to the EFT administration interface, and click the DMZ Gateway tab.

18. In the DMZ Gateway public key section, click the folder and navigate to the certificate that was copied to EFT.

19. Click Apply.
Remote administration via the DMZ Gateway requires that remote administration be enabled on the Server > Administration tab.

DMZ Gateway and EFT are now configured with Secure PNC with mutual authentication

**Secure PNC Settings**

After installing the DMZ Gateway, open gwconfig.xml in the root install folder with a text editor like Notepad. It should have the settings below for each DMZ Gateway profile.

SecurePNCEnabled – This can be set to “true” or “false” to either enable or disable the secure PNC feature. By default this is false. If set to “true” you will also need to at a minimum provide values for the PNCKeystorePath, PNCTrustStorePath, PNCProtocols, and PNCCiphers. If these aren’t set, the DMZGatewayServer.log file should contain log entries explaining what is missing.

If the SecurePNCEnabled setting is set to true, then it also acts like a “require SSL” setting in that only secure peer notification channels will be allowed. In other words, whether or not a channel is to be secured is enforced by the server and not solely dictated by the client.

PNCKeystorePath – The full path to a Java keystore file which contains the certificate and private key (pair) that the DMZ Gateway will use for the PNC. By default, this has no value.

PNCTrustStorePath [Optional] – The full path to a Java keystore (i.e., trust store) file which contains EFT’s certificate (just certificate, not private key) that is specified on the EFT Site-level Connections tab in the SSL Certificate Settings dialog box. If a path is provided, client certificate authentication is required, and therefore EFT’s certificate must exist in this keystore for the certificate to be trusted. If a path is not provided, then client certificate authentication is not required. By default, this has no value.
PNCStorePassphrase – This is that keystore passphrase for both the keystore and truststore mentioned above. You enter the password verbatim and then when the DMZ Gateway starts it will auto-encrypt the passphrase in the config file. By default, this has no value. PNCStorePassphrase is encoded to protect it from casual observance, but for added security it is recommended that you update the ACLs for the gwconfig.xml file to allow read and write access to only the account under which the DMZ Gateway service runs.

PNCProtocols – A comma separated list of protocols that the DMZ Gateway will allow for the secure PNC. This can take on the following values (by default set to TLSv1.2,TLSv1.1):

- TLSv1.2
- TLSv1.1
- TLSv1
- SSLv3 – This protocol is disabled by default by the JRE. To enable it you must update the java.security file under the install folder of the DMZ Gateway under “bin\jre1.8.0_74\lib\security” and remove SSLv3 from the line below:
  - jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA...
- SSLv2Hello

PNCCiphers – Comma-separated list of cipher suites that the DMZ Gateway supports. Defaults to a list of secure ciphers that are supported by Java 1.8. Refer to the “Default Enabled Cipher Suites” section of https://docs.oracle.com/javase/8/docs/technotes/guides/security/SunProviders.html, which shows what Java 8 supports by default irrespective of the default PNCCiphers list.

Per https://docs.oracle.com/javase/7/docs/technotes/guides/security/SunProviders.html#importlimits, Java, by default, limits the encryption strength (i.e., maximum key size) for various algorithms due to import regulations in some countries. Therefore, to use stronger encryption like AES 256, you will need to deploy the JCE Unlimited Strength Jurisdiction Policy Files. We aren’t enabling that by default so that we can make sure we also comply with these import restrictions.

Also, the SSLEngine JCE API doesn’t appear to support the cipher suite syntax such as “RSA+AES” or ! so the full cipher suite names must be specified.

Here is an example of the new config settings with sample values:

```xml
<SecurePNCEnabled>true</SecurePNCEnabled>
<PNCKeyStorePath>C:\devel\certs\keystore.jks</PNCKeyStorePath>
<PNCTrustStorePath>C:\devel\certs\truststore.jks</PNCTrustStorePath>
<PNCStorePassphrase>GSBEvsvavuSo9caA60018fS5B+ubI+zdoDBYtZMoA3vtDQiia65hLnlVldRAwyI2zStqezbnbnsu3E110H5H1Hij9qjQ==</PNCStorePassphrase>
<PNCProtocols>TLSv1.2,TLSv1.1,TLSv1</PNCProtocols>
<PNCCiphers>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256</PNCCiphers>
```

Secure PNC Logging

In most cases, you can inspect the DMZGatewayServer.log for log entries of interest.
For more detailed SSL logging, edit the **DMZGatewayServerService.conf** file by uncommenting this line and restarting the DMZ Gateway server service:

```java
#wrapper.java.additional.6=-Djavax.net.debug=ssl:handshake:data
```

This will print each SSL handshake message to the **DMZGatewayServerService.log** file.

Other options for `javax.net.debug` can be found in [https://docs.oracle.com/javase/6/docs/technotes/guides/security/jsse/JSSERefGuide.html#Debug](https://docs.oracle.com/javase/6/docs/technotes/guides/security/jsse/JSSERefGuide.html#Debug).

It is generally easier to troubleshoot secure PNC communication issues from the perspective of the DMZ Gateway due to the detailed logging that Java offers through that `javax.net.debug` option.

You can also use Wireshark to observe the communication from another perspective and/or to validate that encryption is actually being used on the channel.

### Interface Reference

The topics in this section describe the dialog boxes in DMZ Gateway that have Help buttons and provide a list of frequently used commands.

#### IP Access Exception Entry Dialog Box

Use the **New IP Access Exception Entry** dialog box and the **Edit IP Access Exception Entry** dialog box to provide a specific IP address (e.g., 192.168.43.201) or an IP address mask using wildcards (e.g., 192.168.43.*).

For example, if you want to allow only 192.168.174.159 and block every other IP address, click **Denied access**, click **Add**, then type `192.168.174.159` in the **IP mask** box. This will deny access to all IP addresses **except** 192.168.174.159.

To specify the IP address or mask

1. In the **IP Mask** box, specify the IP address or range of IP addresses to which you are denying or granting access. You can use wildcards to select ranges of IP addresses.
2. Click **OK**. The IP address/mask appears in the exceptions list on the **Access** tab.
**New Profile Wizard--Profile name**

The New Profile Wizard is used to define a new Profile.

In the **Profile Name** box, provide a unique name for this Profile. The name will appear in the interface, logs, error messages, and reports.

**New Profile Wizard--Peer Server Access**

Use the **Peer Server Access** page to specify the IP addresses or IP masks of peer servers who are allowed or denied access to DMZ Gateway. All IP addresses are granted access by default. Refer to **IP Access Exception Dialog Box** for details.
New Profile Wizard--Configuration

Use the Configuration page of the wizard to specify which IP address/port combination on the DMZ Gateway computer should be used as the listening IP addresses.

To specify the client side and server side listening addresses

1. In the Listening IP boxes, click the down arrow to select the IP address or leave the default of All Available. Refer to Specifying the Listening IP Addresses for detailed information.

2. In the Port box, specify the port on which DMZ Gateway communicates with the server. The default is 44500. The connection will be refused if the IP address is on the IP address ban list.