Hosting Laserfiche Forms 10 In A Perimeter Network (DMZ)

White Paper

Laserfiche®

Table of Contents

Introduction

This document provides instructions for configuring Laserfiche Forms 10 in a DMZ. It outlines the following ways to configure Forms for secure access:

1) A standard configuration with two Forms servers and public access to Forms. This involves having a Forms server in the DMZ and another Forms server in the internal network. In the internal network, you can have either a Laserfiche Server with an Active Directory server, or a Laserfiche Directory Server with an STS instance.
2) A version of the standard configuration, but with an additional STS instance in the DMZ. This allows users accessing Forms through a public portal to authenticate to the STS instance in the DMZ, meaning that you do not have to grant these users access to the internal network. This configuration is only possible if Forms authentication goes through Laserfiche Directory Server.
3) A high-security variation on the standard configuration. The main difference with 1) is that there are two SQL Servers rather than one. One SQL Server is in the DMZ and the other is in the internal network.
4) A configuration with only one Forms server, with an STS instance in the DMZ. This configuration is only possible if Forms authentication goes through Laserfiche Directory Server.

Note: When configuring the DMZ, you may need the hardware fingerprint of your machine. You can retrieve the hardware fingerprint using the Hardware Fingerprint Utility on the Forms server machine. A copy of this utility (**showhwfp.exe**) can be found in the Laserfiche Server installation directory, which is C:\Program Files\Laserfiche\Server by default.

Note: For configurations that use two Forms servers, the emails that communicate user task notifications will link to tasks on the internal Forms server by default. If you want your email notifications to link to the Forms server in the DMZ, you should manually alter the value of **FormsHostEmailOverride** in the **cf_options** table in the Forms database. Set the value of this option to http://*DMZFormsServer*/Forms/ to ensure that links in email notifications lead to the public-facing Forms server.

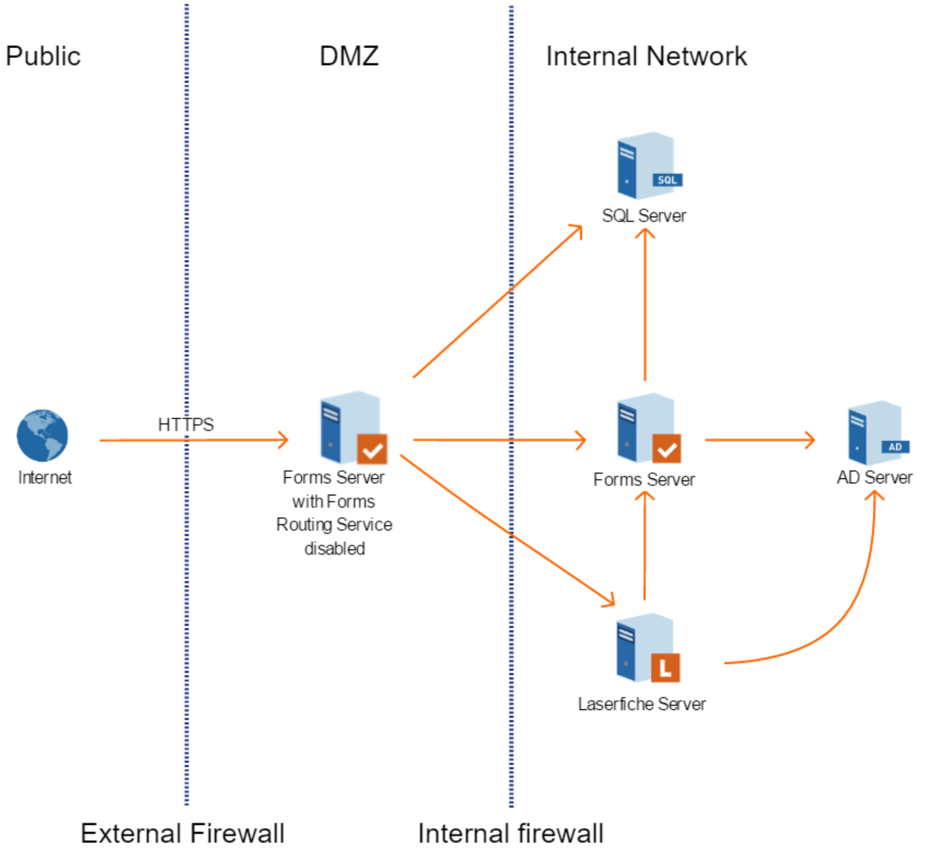
Licensing

Both Forms Essentials and Forms Professional allow for multiple Forms servers. All your Forms servers should have a Forms license of either type. In addition, you will need a Public Portal license to make forms on the DMZ server available to the public. After adding a public portal license, you can then make any form public.

Standard DMZ Configuration: Two Forms Servers, One SQL Server

In the standard configuration, you will install two instances of the Laserfiche Forms server: The primary instance in the internal network, and a second instance in the DMZ. Both instances authenticate to either a Laserfiche Server or a Directory Server STS instance in the internal network. To configure authentication to an STS instance in the DMZ, see the next configuration.

The publicly accessible Forms server located in the DMZ will be able to serve forms to site visitors but will not perform any of the business logic associated with a Forms process. This is because you will disable the routing service for the Forms server located in the DMZ. The internal Forms server is a full installation of Forms. Both Forms servers will point to the same Forms database on SQL Server, located in the internal network.



The DMZ Forms server must be able to communicate with the internal Forms server and the internal SQL Server instance hosting the Forms database. Depending on the authentication method, the DMZ Forms server must also be able to communicate with either a Laserfiche Server instance or a Laserfiche Directory Server instance. The diagram shows a setup with Laserfiche Server authentication and an Active Directory (AD) server. With Laserfiche Directory Server, you would have Laserfiche Directory Server and its STS in the internal network, instead of the AD server.

To configure the DMZ Forms server

In these instructions, we configure the DMZ Forms server to point to the various servers in the internal network and disable the DMZ Forms server's routing service. Before carrying out these instructions, configure the internal Forms server according to the usual instructions.

Where applicable, the instructions will indicate steps that apply to only one method of authentication.

1. Open the Forms configuration site on the DMZ Forms server.
    a. On the **Database** tab, configure the DMZ Forms server to connect to your internal Forms server SQL database.
    b. On the **Forms Server** tab, verify that the configuration matches the internal server.

> **Note:** The Forms configuration site will not be able to validate these settings if the firewall is not configured to allow traffic between the DMZ Forms server and the internal network. See Firewall Considerations for more information.

2. Browse to the DMZ Forms server installation folder and open the **Web.config** file for the Forms configuration site. By default, the file path is

```
C:\Program Files\Laserfiche\Laserfiche Forms\Config\Web.config
```

3. Locate the WCF client configuration block. For the **lfrouting** endpoints, change the **localhost** references to point to your internal Forms server. In the following example, you would replace the bold text in the following sample with the internal Forms server's name.

```
<endpoint address="net.tcp://localhost:8168/lfrouting" binding="netTcpBinding"
bindingConfiguration="timeoutBinding"
contract="Laserfiche.Forms.Routing.IRoutingEngineService" name="" />
```

For Forms 10.3 and later: Also modify the **lflicensing** endpoint to point to the internal Forms server:

```
<endpoint address="net.tcp://localhost:8738/lflicensing"
binding="netTcpBinding" bindingConfiguration="timeoutBinding"
contract="FormsModel.SharedContracts.ILicensingService" name="" />
```

4. **For Laserfiche Forms 10.2.1 and later:** Locate the **<netTcpBinding>** configuration block. Change the security mode from *Transport* to *None*. See the bold text in the following sample.

```
<netTcpBinding>

  <binding name="timeoutBinding" receiveTimeout="00:20:00"
sendTimeout="00:20:00" openTimeout="00:20:00" closeTimeout="00:20:00">

    <security mode="None" />

  </binding>

</netTcpBinding>
```

5. Browse to the DMZ Forms server installation folder and open the **Web.config** file for Forms. By default, the file path is

```
C:\Program Files\Laserfiche\Laserfiche Forms\Forms\Web.config
```

   Then, modify this file according to steps 6-8.

6. Locate the WCF client configuration block. For the **lfrouting**, **lfpushnotification**, **lfautotrigger**, and **lfformexport** endpoints, change the **localhost** references to point to your internal Forms server. In the following example, you would replace the bold sections with the internal Forms server's name.

```
<endpoint address="net.tcp://localhost:8168/lfrouting" binding="netTcpBinding"
          bindingConfiguration="timeoutBinding"
          contract="Laserfiche.Forms.Routing.IRoutingEngineService" name="" />

<endpoint address="net.tcp://localhost:8268/lfpushnotification"
binding="netTcpBinding" bindingConfiguration="timeoutBinding"
contract="Laserfiche.PushNotificationService.SharedContracts.IPushNotification
Service" name="" />

<endpoint address="net.tcp://localhost:8732/lfautotrigger"
binding="netTcpBinding" bindingConfiguration="timeoutBinding"
contract="FormsModel.SharedContracts.IAutoTrigger" name="" />

<endpoint address="net.tcp://localhost:8736/lfformexport"
binding="netTcpBinding" bindingConfiguration="timeoutBinding"
contract="FormsModel.SharedContracts.IFormExportService" name="" />
```

For Forms 10.3 and later: also modify the **lflicensing** endpoint to point to the internal Forms server:

```
<endpoint address="net.tcp://localhost:8738/lflicensing"
binding="netTcpBinding" bindingConfiguration="timeoutBinding"
contract="FormsModel.SharedContracts.ILicensingService" name="" />
```

7. *If you are using the Laserfiche Directory Server STS:*
   a. Locate the **wsFederation** node. It should begin with the string <wsFederation persistentCookiesOnPassiveRedirects=.
   b. In the **wsFederation** node, change the **realm** and **reply** attributes to the address of the DMZ Forms server.
   c. In the same node, change the **issuer** variable to the location of the Laserfiche Directory Server STS in the internal network.
8. **For Laserfiche Forms 10.2.1 and later:** Locate the **<netTcpBinding>** configuration block. Change the security mode from *Transport* to *None*. See the bold text in the following sample.

```
<netTcpBinding>

 <binding name="timeoutBinding" receiveTimeout="00:59:00"
sendTimeout="00:59:00" openTimeout="00:59:00" closeTimeout="00:59:00">

  <security mode="None" />

 </binding>

</netTcpBinding>
```

9. Open the Windows Services Microsoft Management Console (MMC) snap-in.
   a. View the properties of the **Laserfiche Forms Routing Service** to **Stop** the service and change the **Startup type** to **Disabled**.
   b. View the properties of the **Laserfiche Notification Hub Service** to **Stop** the service and change the startup type to **Disabled**.
   c. View the properties of the **Laserfiche Notification Master Service** to **Stop** the service and change the startup type to **Disabled**.

To configure the internal Forms server

For Laserfiche Forms 10.2.1 and later:

1. Browse to the internal Forms server installation folder and open the **Web.config** file. By default, the file path is

```
C:\Program Files\Laserfiche\Laserfiche Forms\Forms\Web.config
```

2. Locate the **<netTcpBinding>** configuration block. Change the security mode from *Transport* to *None*. See the bold text in the following sample.

```
<netTcpBinding>
  <binding name="timeoutBinding" receiveTimeout="00:59:00"
sendTimeout="00:59:00" openTimeout="00:59:00" closeTimeout="00:59:00">
    <security mode="None" />
  </binding>
</netTcpBinding>
```

3. Browse to the internal Forms server installation folder and open the **RoutingEngineServiceHost.exe.config** file. By default, the file path is

```
C:\Program Files\Laserfiche\Laserfiche
Forms\Forms\bin\RoutingEngineServiceHost.exe.config
```

4. Locate the **<netTcpBinding>** configuration block. Change the security mode from *Transport* to *None*. See the bold text in the following sample.

```
<netTcpBinding>
  <binding name="timeoutBinding" receiveTimeout="00:59:00"
sendTimeout="00:59:00" openTimeout="00:59:00" closeTimeout="00:59:00"
maxReceivedMessageSize="200000000">
    <security mode="None" />
  </binding>
</netTcpBinding>
```

5. Browse to the **Web.config** file for the Forms configuration site. By default, the file path is

```
C:\Program Files\Laserfiche\Laserfiche Forms\Config\Web.config
```

Locate the **<netTcpBinding>** configuration block. Change the security mode from *Transport* to *None*. See the bold text in the following sample.

```
<netTcpBinding>
  <binding name="timeoutBinding" receiveTimeout="00:20:00"
sendTimeout="00:20:00" openTimeout="00:20:00" closeTimeout="00:20:00">
    <security mode="None" />
  </binding>
</netTcpBinding>
```

6. Browse to the **Laserfiche.PushNotificationService.Master.Host.exe.config** file for the internal Notification service. By default, the file path is

   ```
   C:\Program Files (x86)\Laserfiche\Laserfiche
   Notification\Service\Laserfiche.PushNotificationService.Master.Host.exe.config
   ```

7. Locate the <netTcpBinding> configuration block. Change the security mode from Transport to None. See the bold text in the following sample.

   ```
   <netTcpBinding>

     <binding name="timeoutBinding" receiveTimeout="00:20:00"
   sendTimeout="00:59:00" openTimeout="00:59:00" closeTimeout="00:59:00"
   maxReceivedMessageSize="200000000">

       <security mode="None" />

     </binding>

   </netTcpBinding>
   ```

Two Forms Servers with Two STS Instances

This configuration works only if you are using Laserfiche Directory Server. It is identical to the standard configuration, except that the DMZ Forms server authenticates to an STS instance in the DMZ, while there is a separate STS instance in the internal network for the primary Forms server to authenticate to. To accommodate having an STS instance on a different computer from the Directory Server computer, we have to change the endpoints in the DMZ Forms server.

> **Note:** In order for the STS instance in the DMZ to authenticate to the Directory Server in the internal network, the DMZ server must have a valid SSL certificate.

Before carrying out these instructions, configure the internal Forms server according to the usual instructions.

To configure the DMZ Forms server

1. Configure the internal Forms server using the default configuration instructions.
2. Configure the firewall to open ports between the DMZ Forms server and the following internal servers: Laserfiche Directory Server, the internal Forms server, and the Forms SQL Server. See Firewall Considerations for more information.
3. Give **FormsAppPool** full control permission to the private key in the certificate used by the Forms site.
    a. Open **Microsoft Management Console (MMC)**. If the snap-in for Certificates is not installed, install it by going to **File,** selecting **Add/Remove Snap-in**, and selecting the **Certificates** snap-in. Choose to add this snap-in for the **Local Computer**.
    b. Once the snap-in is added, click on **Certificates** in the left pane, and within this, on **Personal**.
    c. If you have created a certificate for the Forms site and saved it to the **Personal** node, there will be a subfolder in this node labeled **Certificates**. Expand this.
    d. Right-click on the certificate for the Forms site. Select **All Tasks**, then **Manage private keys**.

    e. Select **Add…** under the "Group or user names" section. In the ensuing dialog box, enter the object names to be added. Choose the location to be the local computer. Then check for the object name **IIS AppPool\FormsAppPool**. After the object is found, click **OK**.
    f. Back in the permissions for private keys dialog box, select **FormsAppPool** in the "Group or user names" section. In the "Permissions for FormsAppPool" section, ensure that **Allow** is checked for the option **Full control**. Click **OK** to save this setting.

4. Find the **EndpointUtility.exe** program in the Forms installation folder (by default, it is in C:\Program Files\Laserfiche\Laserfiche Forms\Forms\bin). Open **EndpointUtility.exe**, and configure the endpoints as follows:
    a. Enter the Forms installation path. By default, this is C:\Program Files\Laserfiche\Laserfiche Forms.
    b. For **Laserfiche Directory Server Address**, enter the fully qualified domain name for the Laserfiche Directory Server.
    c. Select **Use Alternative Service**. Select **Certificate** as the security mode. From the list of certificates presented, choose the certificate used for the Forms site.
    d. Click **Save** to update all related configuration files.
5. Open the Forms configuration site on the DMZ Forms server.
    a. On the **Database** tab, configure the DMZ Forms server to connect to your Forms SQL database.
6. Browse to the DMZ Forms server installation folder and open the **Web.config** file for the Forms configuration site. By default, the file path is

    ```
    C:\Program Files\Laserfiche\Laserfiche Forms\Config\Web.config
    ```

7. Locate the WCF client configuration block. For the **lfrouting** endpoints, change the **localhost** references to point to your internal Forms server. In the following example, you would replace the bold sections in the following sample with the internal Forms server's name.

    ```
    <endpoint address="net.tcp://localhost:8168/lfrouting" binding="netTcpBinding"
    bindingConfiguration="timeoutBinding"
    contract="Laserfiche.Forms.Routing.IRoutingEngineService" name="" />
    ```

    For Forms 10.3 and later: also modify the **lflicensing** endpoint to point to the internal Forms server:

    ```
    <endpoint address="net.tcp://localhost:8738/lflicensing"
    binding="netTcpBinding" bindingConfiguration="timeoutBinding"
    contract="FormsModel.SharedContracts.ILicensingService" name="" />
    ```

8. **For Laserfiche Forms 10.2.1 and later:** Locate the **<netTcpBinding>** configuration block. Change the security mode from *Transport* to *None*. See the bold text in the following sample.

```
<netTcpBinding>
  <binding name="timeoutBinding" receiveTimeout="00:20:00"
sendTimeout="00:20:00" openTimeout="00:20:00" closeTimeout="00:20:00">
    <security mode="None" />
  </binding>
</netTcpBinding>
```

9. Browse to the DMZ Forms server installation folder and open the **Web.config** file. By default, the file path is

```
C:\Program Files\Laserfiche\Laserfiche Forms\Forms\Web.config
```

   a. Locate the WCF client configuration block. For the **lfrouting**, **lfpushnotification**, **lfautotrigger**, and **lfformexport** endpoints, change the **localhost** references to point to your internal Forms server. In the following example, you would replace the bold sections in the following sample with the internal Forms server's name.

```
<endpoint address="net.tcp://localhost:8168/lfrouting"
binding="netTcpBinding" bindingConfiguration="timeoutBinding"
contract="Laserfiche.Forms.Routing.IRoutingEngineService" name="" />

<endpoint address="net.tcp://localhost:8732/lfautotrigger"
binding="netTcpBinding" bindingConfiguration="timeoutBinding"
contract="FormsModel.SharedContracts.IAutoTrigger" name="" />

<endpoint address="net.tcp://localhost:8268/lfpushnotification"
binding="netTcpBinding" bindingConfiguration="timeoutBinding"
contract="Laserfiche.PushNotificationService.SharedContracts.IPushNotificationService" name="" />

<endpoint address="net.tcp://localhost:8736/lfformexport"
binding="netTcpBinding" bindingConfiguration="timeoutBinding"
contract="FormsModel.SharedContracts.IFormExportService" name="" />
```

   b. Locate the **wsFederation** node. It should begin with the string <wsFederation persistentCookiesOnPassiveRedirects=.

   c. In the **wsFederation** node, change the **realm** and **reply** variables to the address of the DMZ Forms server.

    d. In the same node, change the **issuer** variable to the location of the Laserfiche Directory Server STS in the DMZ.

    e. **For Laserfiche Forms 10.2.1 and later:** Locate the **<netTcpBinding>** configuration block. Change the security mode from *Transport* to *None*. See the bold text in the following sample.

    ```
    <netTcpBinding>
      <binding name="timeoutBinding" receiveTimeout="00:20:00"
    sendTimeout="00:20:00" openTimeout="00:20:00" closeTimeout="00:20:00">
        <security mode="None" />
      </binding>
    </netTcpBinding>
    ```

10. Open **Microsoft Management Console (MMC)**. Add the **Services** snap-in if it does not already exist. This can be done by clicking on **File**, then choosing **Add/Remove Snap-in**. Once you have the snap-in, perform the following steps:
    a. Select **Services** in the left pane.
    b. In the list of services, right-click on **Laserfiche Forms Routing Service** and select **Properties**. Choose to **Stop** the service, then change the **Startup type** to **Disabled**.
    c. In the list of services, right-click on **Laserfiche Notification Hub Service**. Choose to **Stop** the service, then change the startup type to **Disabled**.
    d. In the list of services, right-click on **Laserfiche Notification Master Service.** Choose to **Stop** the service, then change the startup type to **Disabled**.

To configure the internal Forms server

For Laserfiche Forms 10.2.1 and later:

1. Browse to the internal Forms server installation folder and open the **Web.config** file. By default, the file path is:

   ```
   C:\Program Files\Laserfiche\Laserfiche Forms\Forms\Web.config
   ```

2. Locate the **<netTcpBinding>** configuration block. Change the security mode from *Transport* to *None*. See the bold text in the following sample.

   ```
   <netTcpBinding>
     <binding name="timeoutBinding" receiveTimeout="00:59:00"
   sendTimeout="00:59:00" openTimeout="00:59:00" closeTimeout="00:59:00">
       <security mode="None" />
     </binding>
   </netTcpBinding>
   ```

3. Browse to the internal Forms server installation folder and open the **RoutingEngineServiceHost.exe.config** file. By default, the file path is:

   ```
   C:\Program Files\Laserfiche\Laserfiche
   Forms\Forms\bin\RoutingEngineServiceHost.exe.config
   ```

4. Locate the **<netTcpBinding>** configuration block. Change the security mode from *Transport* to *None*. See the bold text in the following sample.

   ```
   <netTcpBinding>
     <binding name="timeoutBinding" receiveTimeout="00:59:00"
   sendTimeout="00:59:00" openTimeout="00:59:00" closeTimeout="00:59:00"
   maxReceivedMessageSize="200000000">
       <security mode="None" />
     </binding>
   </netTcpBinding>
   ```

5. Browse to the **Web.config** file for the Forms Configuration site. By default, the file path is:

   ```
   C:\Program Files\Laserfiche\Laserfiche Forms\Config\Web.config
   ```

   Locate the **<netTcpBinding>** configuration block. Change the security mode from *Transport* to *None*. See the bold text in the following sample.

   ```
   <netTcpBinding>
     <binding name="timeoutBinding" receiveTimeout="00:20:00"
   sendTimeout="00:20:00" openTimeout="00:20:00" closeTimeout="00:20:00">
       <security mode="None" />
     </binding>
   </netTcpBinding>
   ```

6. Browse to the **Laserfiche.PushNotificationService.Master.Host.exe.config** file for the internal Notification service. By default, the file path is

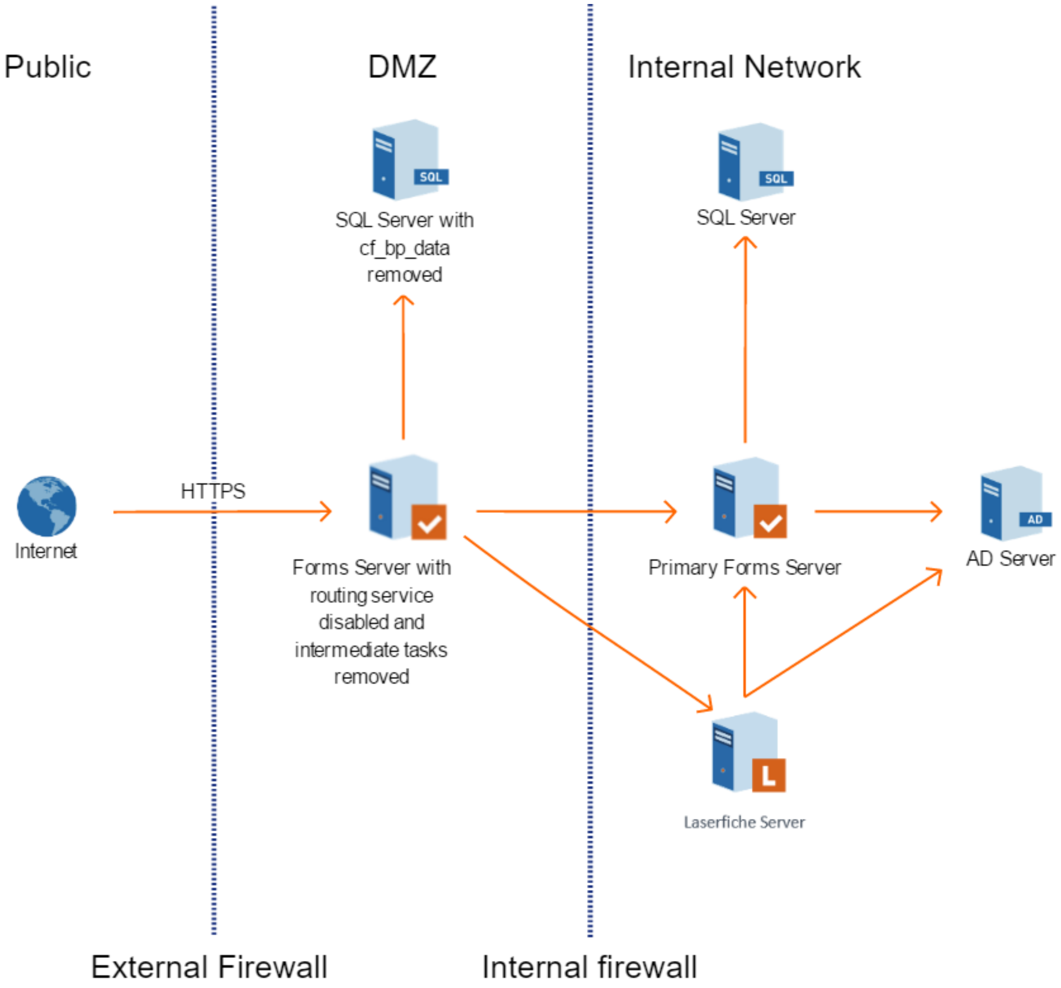
```
C:\Program Files (x86)\Laserfiche\Laserfiche Notification\Service\Laserfiche.PushNotificationService.Master.Host.exe.config
```

7. Locate the <netTcpBinding> configuration block. Change the security mode from Transport to None. See the bold text in the following sample.

```
<netTcpBinding>
  <binding name="timeoutBinding" receiveTimeout="00:20:00"
sendTimeout="00:59:00" openTimeout="00:59:00" closeTimeout="00:59:00"
maxReceivedMessageSize="200000000">
    <security mode="None" />
  </binding>
</netTcpBinding>
```

High-Security Variation: Two Forms Servers, Two SQL Servers

This configuration is like the standard configuration, except that there are two SQL Server instances rather than one. An additional copy of the Forms database is in the DMZ with the DMZ Forms server. The DMZ Forms server does not communicate with the Forms SQL Server on the internal network. The SQL database in the DMZ stores the blank starting form definitions, but is scrubbed of process data.



In this configuration, a public user accessing Forms through the internet can only submit a form (without file uploads) or start a process. They cannot do anything else through a public connection.

Note: Users accessing the form through the DMZ Forms server cannot upload files with the form unless you open port 1433 in the internal firewall and configure SQL transactional replication for a specific table in the Forms database. For more details, see Synchronizing attachments.

This configuration is possible with both Laserfiche Server authentication and Laserfiche Directory Server authentication. Where applicable, the instructions will indicate steps that apply to only one method of authentication.

To configure the DMZ Forms server

In these instructions, we configure the DMZ Forms server to connect to the appropriate servers in the DMZ and the internal network. We also set up the DMZ SQL database and purge the relevant information from it and the DMZ Forms server. Finally, we turn off the DMZ Forms server's routing service.

Before carrying out these instructions, configure the internal Forms server according to the usual instructions.

1. Create the DMZ Forms SQL database as follows.
    a. Make a copy of the internal Forms SQL database.
    b. Clear the **cf_bp_data** table in the copied database. This table stores data from the fields in submitted forms, and we want to make sure that no information is leaked even if the DMZ is compromised.
    c. Move the copied database to the DMZ machine.
    d. On the Forms configuration site for the DMZ Forms server, configure the DMZ Forms server to connect to the DMZ SQL database.
    e. Modify all Forms process diagrams in the DMZ Forms server to have only a message start event and an end event. This way, the structure of tasks will not be revealed even if the DMZ is compromised. This action also deletes all tasks in the Forms inbox.
    f. Close any open SQL connections going through the internal firewall.
2. Open the Forms configuration site on the DMZ Forms server.
    a. On the **Forms Server** tab, specify the internal Forms server URL.
    If you are using Laserfiche Server for authentication:
        i. On the **User Authentication** tab, select **Use Laserfiche Server authentication** and specify the internal Laserfiche Server host name. If Laserfiche Server is not running on port 80, make sure to specify the port value in the host name in the format *ServerName*:*PortNumber*.

If you are using Laserfiche Directory Server for authentication:

ii. On the **User Authentication** tab, select **Use a Laserfiche Directory Server for Single Sign-On authentication** and specify the fully qualified domain name of the Laserfiche Directory Server STS in the internal network, in the format //*DirectoryServer*/LFDSSTS. Specify the internal Directory Server's database.

b. On the **Email Settings** tab, specify your SMTP server for draft notifications. If the SMTP email server is on the internal network, you will have to allow the DMZ Forms server to communicate with your email server. If the DMZ Forms server cannot access the email server, users can still save drafts, but they will not receive email notifications of the drafts.

3. Browse to the DMZ Forms server installation folder and open the **Web.config** file for the Forms configuration site. By default, the file path is

   ```
   C:\Program Files\Laserfiche\Laserfiche Forms\Config\Web.config
   ```

4. Locate the WCF client configuration block. For the **lfrouting** endpoints, change the **localhost** references to point to your internal Forms server. In the following example, you would replace the bold text in the following sample with the internal Forms server's name.

   ```
   <endpoint address="net.tcp://localhost:8168/lfrouting" binding="netTcpBinding"
   bindingConfiguration="timeoutBinding"
   contract="Laserfiche.Forms.Routing.IRoutingEngineService" name="" />
   ```

   For Forms 10.3 and later: also modify the **lflicensing** endpoint to point to the internal Forms server:

   ```
   <endpoint address="net.tcp://localhost:8738/lflicensing"
   binding="netTcpBinding" bindingConfiguration="timeoutBinding"
   contract="FormsModel.SharedContracts.ILicensingService" name="" />
   ```

5. **For Laserfiche Forms 10.2.1 and later:** Locate the **<netTcpBinding>** configuration block. Change the security mode from *Transport* to *None*. See the bold text in the following sample.

   ```
   <netTcpBinding>

     <binding name="timeoutBinding" receiveTimeout="00:20:00"
   sendTimeout="00:20:00" openTimeout="00:20:00" closeTimeout="00:20:00">

       <security mode="None" />

     </binding>

   </netTcpBinding>
   ```

6. Browse to the DMZ Forms server installation folder and open the **Web.config** file for Forms. By default, the file path is

```
C:\Program Files\Laserfiche\Laserfiche Forms\Forms\Web.config
```

7. Locate the WCF client configuration block. For the **lfrouting**, **lfpushnotification**, **lfautotrigger**, and **lfformexport** endpoints, change the **localhost** references to point to your internal Forms server. In the following example, you would replace the bold sections in the following sample with the internal Forms server's name.

```
<endpoint address="net.tcp://localhost:8168/lfrouting" binding="netTcpBinding"
bindingConfiguration="timeoutBinding"
contract="Laserfiche.Forms.Routing.IRoutingEngineService" name="" />

<endpoint address="net.tcp://localhost:8268/lfpushnotification"
binding="netTcpBinding" bindingConfiguration="timeoutBinding"
contract="Laserfiche.PushNotificationService.SharedContracts.IPushNotification
Service" name="" />

<endpoint address="net.tcp://localhost:8732/lfautotrigger"
binding="netTcpBinding" bindingConfiguration="timeoutBinding"
contract="FormsModel.SharedContracts.IAutoTrigger" name="" />

<endpoint address="net.tcp://localhost:8736/lfformexport"
binding="netTcpBinding" bindingConfiguration="timeoutBinding"
contract="FormsModel.SharedContracts.IFormExportService" name="" />
```

For Forms 10.3 and later: also modify the **lflicensing** endpoint:

```
<endpoint address="net.tcp://localhost:8738/lflicensing"
binding="netTcpBinding" bindingConfiguration="timeoutBinding"
contract="FormsModel.SharedContracts.ILicensingService" name="" />
```

8. *If you are using the Laserfiche Directory Server STS:*
   a. Locate the **wsFederation** node. It should begin with the string `<wsFederation persistentCookiesOnPassiveRedirects=`.
   b. In the **wsFederation** node, change the **realm** and **reply** attributes to the address of the DMZ Forms server.
   c. In the same node, change the **issuer** variable to the location of the Laserfiche Directory Server STS in the internal network.

9. **For Laserfiche Forms 10.2.1 and later:** Locate the **<netTcpBinding>** configuration block. Change the security mode from *Transport* to *None*. See the bold text in the following sample.

   ```
   <netTcpBinding>
     <binding name="timeoutBinding" receiveTimeout="00:59:00"
   sendTimeout="00:59:00" openTimeout="00:59:00" closeTimeout="00:59:00">
       <security mode="None" />
     </binding>
   </netTcpBinding>
   ```

10. Open the Windows Services Microsoft Management Console (MMC) snap-in
    - d. View the properties of the **Laserfiche Forms Routing Service** to **Stop** the service and change the **Startup type** to **Disabled**.
    - e. View the properties of the **Laserfiche Notification Hub Service** to **Stop** the service and change the startup type to **Disabled**.
    - f. View the properties of the **Laserfiche Notification Master Service** to **Stop** the service and change the startup type to **Disabled**.

To configure the internal Forms server

For Laserfiche Forms 10.2.1 and later:

1. Browse to the internal Forms server installation folder and open the **Web.config** file. By default, the file path is

   ```
   C:\Program Files\Laserfiche\Laserfiche Forms\Forms\Web.config
   ```

2. Locate the **<netTcpBinding>** configuration block. Change the security mode from *Transport* to *None*. See the bold text in the following sample.

   ```
   <netTcpBinding>
     <binding name="timeoutBinding" receiveTimeout="00:59:00"
   sendTimeout="00:59:00" openTimeout="00:59:00" closeTimeout="00:59:00">
       <security mode="None" />
     </binding>
   </netTcpBinding>
   ```

3. Browse to the internal Forms server installation folder and open the **RoutingEngineServiceHost.exe.config** file. By default, the file path is

   ```
   C:\Program Files\Laserfiche\Laserfiche
   Forms\Forms\bin\RoutingEngineServiceHost.exe.config
   ```

4. Locate the **<netTcpBinding>** configuration block. Change the security mode from *Transport* to *None*. See the bold text in the following sample.

   ```
   <netTcpBinding>
     <binding name="timeoutBinding" receiveTimeout="00:59:00"
   sendTimeout="00:59:00" openTimeout="00:59:00" closeTimeout="00:59:00"
   maxReceivedMessageSize="200000000">
       <security mode="None" />
     </binding>
   </netTcpBinding>
   ```

5. Browse to the **Web.config** file for the Forms Configuration site. By default, the file path is

   ```
   C:\Program Files\Laserfiche\Laserfiche Forms\Config\Web.config
   ```

   Locate the **<netTcpBinding>** configuration block. Change the security mode from *Transport* to *None*. See the bold text in the following sample.

   ```
   <netTcpBinding>
     <binding name="timeoutBinding" receiveTimeout="00:20:00"
   sendTimeout="00:20:00" openTimeout="00:20:00" closeTimeout="00:20:00">
       <security mode="None" />
     </binding>
   </netTcpBinding>
   ```

6. Browse to the **Laserfiche.PushNotificationService.Master.Host.exe.config** file for the internal Notification service. By default, the file path is

   ```
   C:\Program Files (x86)\Laserfiche\Laserfiche
   Notification\Service\Laserfiche.PushNotificationService.Master.Host.exe.config
   ```

7. Locate the <netTcpBinding> configuration block. Change the security mode from Transport to None. See the bold text in the following sample.

```
<netTcpBinding>
  <binding name="timeoutBinding" receiveTimeout="00:20:00"
sendTimeout="00:59:00" openTimeout="00:59:00" closeTimeout="00:59:00"
maxReceivedMessageSize="200000000">
    <security mode="None" />
  </binding>
</netTcpBinding>
```

Note: In this configuration, the submitted form will not show up on the Thank You page. This protects the submitted data. The Thank You page retrieves its data after the routing engine finishes submitting the form, so this data cannot be accessed. You should direct users to your own custom Thank You page.

Note: Because the intermediate steps in processes have been purged on the DMZ Forms server, only changes in the start event in the DMZ Forms server's process modeler will affect the actual process. Any changes made in the DMZ Forms server to events after the start event will have no effect on the internal Forms server.

Note: Timer start events will work only on the internal Forms server.

Note: If your processes do not change, your DMZ SQL Server does not need to be updated with data from the internal servers. If you update existing processes or add new processes in the internal Forms server, you can push these out to the DMZ SQL Server using one of two methods. The first method is to simply copy the internal SQL Server to the DMZ again, following step 1 in To configure the DMZ Forms server. The second method is to export the relevant processes (in XML format) from the internal Forms server and import them to the DMZ Forms server. After import, modify the processes so that they have only a message start event and an end event. The second method is only possible with Forms 10.3 and later.

Synchronizing attachments

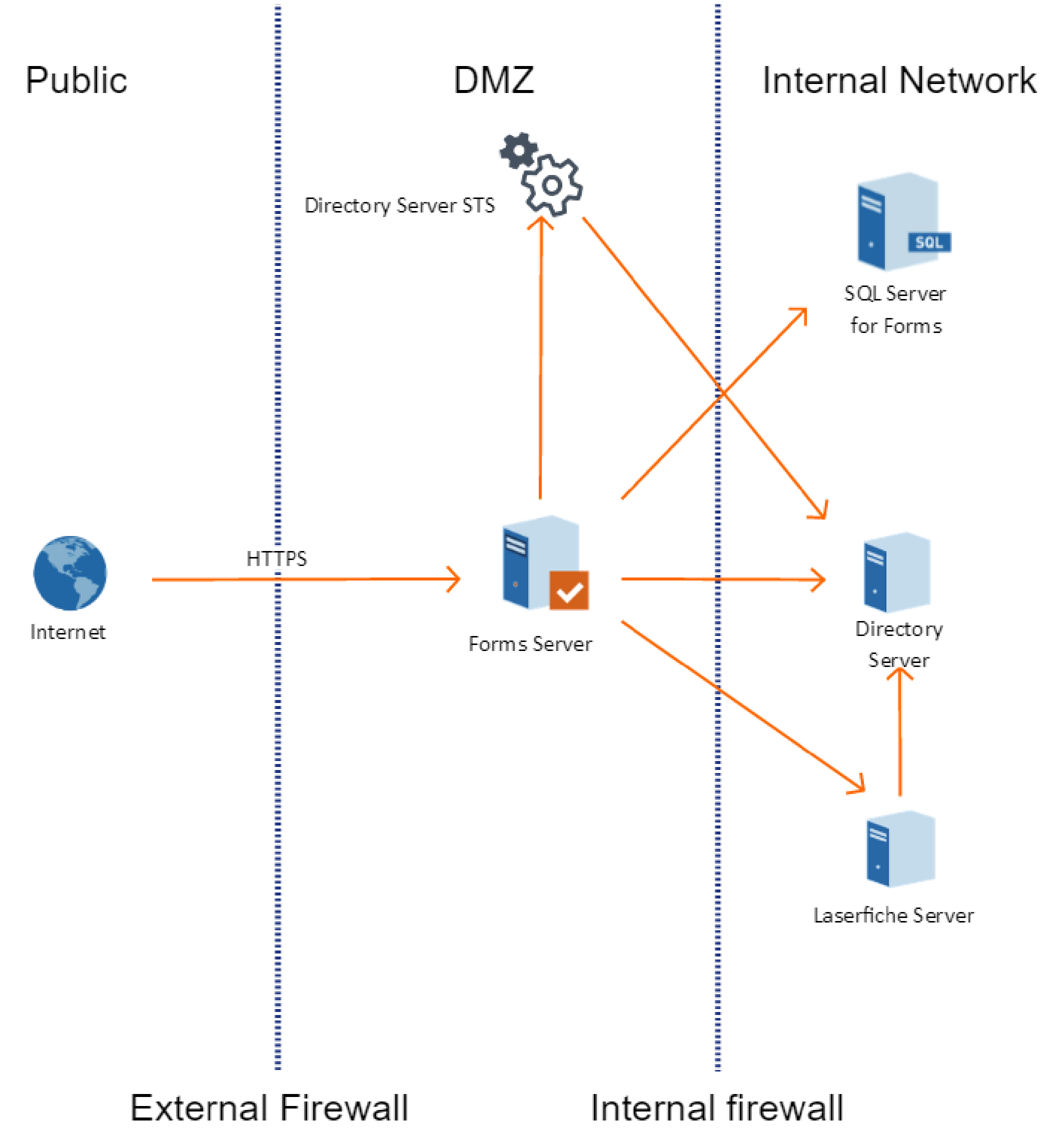
By default, in a setup with two distinct SQL Servers, users submitting forms to the DMZ Forms server cannot upload attachments as part of the form. To enable attachment submission from the DMZ, configure SQL transactional replication for the attachments table. Note that this requires opening a port, which decreases the security of your setup.

To replicate attachments from the DMZ database to the internal database

1. Make sure port 1433 on the internal SQL Server is open for inbound traffic.
2. Once both databases have been created, follow Microsoft's instructions on configuring transactional replication to make the DMZ database a publisher and the internal database a subscriber.
3. Publish the **cf_bp_attachment_data** table. For security, do not publish any other tables.

One Forms Server in DMZ

This configuration uses only one Forms server, located in the DMZ. A Laserfiche Directory Server STS instance should be installed in the DMZ. Laserfiche Directory Server and the Forms SQL Server should be installed in the internal network.



Note: In order for the STS instance in the DMZ to authenticate to the Directory Server in the internal network, the DMZ server must have a valid certificate.

To configure the DMZ Forms server

In these instructions, we configure the DMZ Forms server to connect to the relevant servers in the DMZ and the internal network. We then configure the DMZ Forms server to authenticate to the Laserfiche Directory Server STS in the DMZ.

1. Configure the firewall to open the appropriate ports between the DMZ Forms server and the following servers in the internal network: Laserfiche Directory Server, Laserfiche Server, and SQL Server.
2. Carry out Steps 3-4 in the earlier instructions for configuring the DMZ Forms server when there are two STS instances.
3. Open the Forms configuration site on the DMZ Forms server.
    a. On the **Database** tab, configure the DMZ Forms server to connect to your server SQL database.
    b. On the **User Authentication** tab, select **Use a Laserfiche Directory Server for Single Sign-On authentication** and set **Directory Server STS URL** to the address of the Laserfiche Directory Server STS in the DMZ.

Firewall Considerations

The DMZ Forms server must be able to communicate with the internal computers hosting the following services:

- The internal Forms server, if you are using one of the configurations with two Forms servers.
- The Microsoft SQL Server instance hosting the Forms SQL database.
- Either the Laserfiche Server or Directory Server, depending on your Forms authentication method.

When opening ports in the firewall, make sure to only allow connections from the DMZ Forms server.

Internal Forms Server

When modifying the DMZ Forms server **Web.config** files, take note of the port values specified for the various endpoints. The DMZ Forms server must be able to communicate with the internal Forms server on these ports.

SQL Server

Forms must also be able to communicate with the appropriate SQL Server. Make sure that the appropriate SQL Server port (the default port is 1433) is open to traffic from the appropriate Forms server.

If the DMZ Forms server is configured to use Laserfiche Server authentication

The DMZ Forms server must be able to communicate with your internal Laserfiche Server. By default, Laserfiche Server uses port 80 for unsecured traffic, port 443 for secure traffic, and port 5051 for Laserfiche Server notifications.

If the DMZ Forms server is configured to use Laserfiche Directory Server authentication

The DMZ Forms server must be able to communicate with Laserfiche Directory Server. By default, Directory Server uses port 5048 for unsecured traffic and port 5049 for secure traffic. This information is embedded in the Forms license file. By default, the Forms license file is located at

```
C:\Program Files\Laserfiche\Laserfiche Forms\Forms\bin\lf.licx
```

Open the file and locate the **LicenseServerListeningPort** value.

Email Server

If the SMTP email server is on the internal network, you will have to allow the DMZ Forms server to communicate with your SMTP email server. If the DMZ Forms server cannot access the SMTP email server, users can still save drafts from DMZ Forms server, but they will not receive email notifications of the drafts.

Summary of common ports

Product	Ports
Forms 10	80 for HTTP, 443 for HTTPS 8168 for lfrouting 8268 for lfpushnotification 8181 for the Notification Hub Service 8732 for lfautotrigger 8736 for lfformexport 8738 for lflicensing (Forms 10.3 and later)
Directory Server 10	5048 for HTTP 5049 for HTTPS
Laserfiche Server 10	80 for HTTP 443 for HTTPS 5051 for notifications
Microsoft SQL Server	1433 for default instance
SMTP Server	25 for default SMTP port

Hosting Laserfiche Forms 10 In A Perimeter Network (DMZ)
September 2018

Author: Leif Hancox-Li
Editor: Roger Wu
Technical Editor: Xiang Xiuhong, Alexander Huang

Description:
This paper covers general configuration considerations when hosting Laserfiche Forms in a DMZ.

Laserfiche
3545 Long Beach Blvd.
Long Beach, CA 90807
U.S.A

Phone: +1.562.988.1688
www.laserfiche.com

Compulink Management Center, Inc. makes no representations or warranties with respect to the contents or use of this manual, and specifically disclaims any express or implied warranties, merchantability, or fitness for any particular purpose. Furthermore, Compulink Management Center, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.