**TLS 1.2 Implementation**

**STEP 1:**

### **Binding Host Certificates in IIS (Internet Information Services)**

Laserfiche web applications run on IIS, Microsoft’s web server. IIS is an optional feature of Windows Server 2016 that you will need to enable.

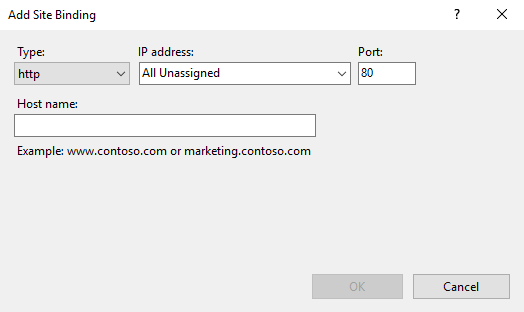
Install the most recent version of IIS on each Laserfiche server except the SQL server, Quick Fields, and Distributing Computing Cluster VMs. Then, perform the following steps to bind the host certificate to port 443. This will enable secure connections on port 443 using TLS 1.2. This can be done before or after installing Laserfiche products.

1. From the IIS Manager, in the **Connections** pane, expand the server name, expand **Sites**, and then select **Default Web Site.**
2. In the **Actions** pane, select **Bindings**.

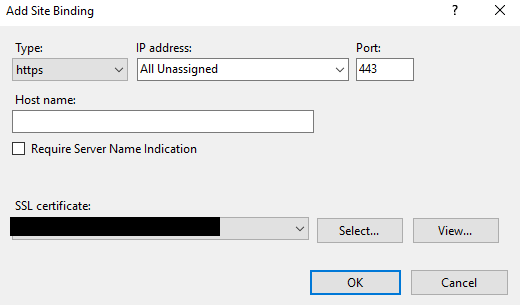
The **Site Bindings** window appears.

1. Select **Add.**

Information similar to the following appears:



1. In the **Type** list, select **https**. The **Port** box is automatically populated with **443.**
2. In the **SSL certificate** list, select the certificate with the FQDN of the server.



1. Select **OK**.
2. Select **Close.** You are finished with this procedure.

**STEP 2:**

### **Enabling TLS 1.2 – Workflow servers, Forms servers**

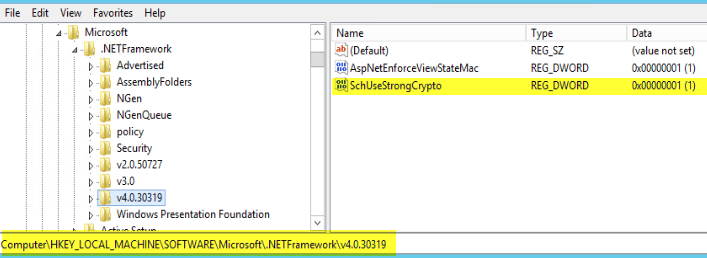
Some Laserfiche products use older .Net libraries that do not support TLS 1.2. Enable TLS 1.2 for Workflow and Forms by updating the registry. This can be done before or after installing Laserfiche products.

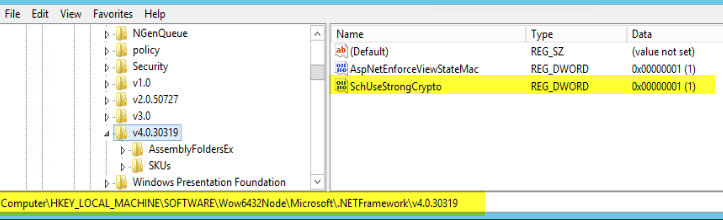
To update the registry, perform the following steps:

1. Make a backup of your registry.
2. Open PowerShell as administrator.
3. In the PowerShell window, paste the following commands:

|  |
| --- |
| #Make directory for registry backups  $sourcePath = "C:\Source"  $regBackupPath = $sourcePath + "\RegistryBackups\" + (Get-Date -format "yyyy-MM-dd HHmm ss") + "\"  New-Item -ItemType Directory -Force -Path $regBackupPath $regBackupPath = $sourcePath + "\RegistryBackups\" + (Get-Date -format "yyyy-MM-dd HHmm ss") + "\"  Reg export HKLM\SOFTWARE\Microsoft\.NetFramework\v4.0.30319 ($regBackupPath + "\HKLM-SOFTWARE-CurrentControlSet-Microsoft-.NetFramework-v4.0.30319.reg") New-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\.NetFramework\v4.0.30319' -Name 'SchUseStrongCrypto' -Value '1' -PropertyType 'DWord' -Force | Out-Null Set-ItemProperty -Path 'HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NetFramework\v4.0.30319' -Name 'SchUseStrongCrypto' -Value '1' -Force | Out-Null Write-Host 'TLS 1.2 has been enabled in .NET Framework.' |

1. Restart the server.





**STEP 3:**

### **Binding Other Certificates – LFS Servers, Forms Servers**

!!IMPORTANT!! In some cases, certificates have to be bound to ports manually.

**Note:** This must be done *after* installing Laserfiche Server.

Create a GUID: <https://www.guidgenerator.com/>

#### **Laserfiche Server (LFS)**

Log in to the host running Laserfiche Server. Open an administrative PowerShell window. Bind the SSL certificate to port 443 by typing:

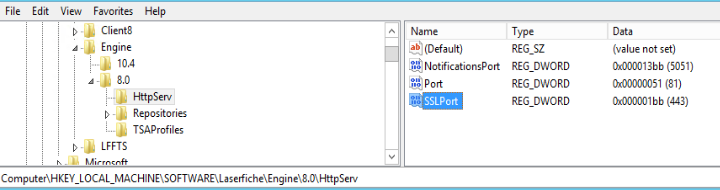
|  |
| --- |
| netsh http add sslcert ipport=0.0.0.0:443 certhash=<*x*> appid={<*n*>} |

Where <*x*> is the server certificate thumbprint and <*n*> is a valid GUID.

**STEP 4:**

**Workflow only** : Then, set the SSL port registry key by typing:

|  |
| --- |
| New-ItemProperty -Path 'HKLM:\SOFTWARE\Laserfiche\Engine\8.0\HttpServ' -Name 'SSLPort' -Value '443' -PropertyType 'DWord' -Force | Out-Null |



For more information on this topic, see [Using SSL/TLS with Laserfiche](https://www.laserfiche.com/support/webhelp/Laserfiche/10/en-us/administration/#../Subsystems/LFAdmin/Content/Using_SSL_TLS.htm).

**STEP 5:**

For information on how to find the certificate thumbprint, see [How to: Retrieve the Thumbprint of a Certificate](https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/how-to-retrieve-the-thumbprint-of-a-certificate). To find a GUID, use PowerShell, the [Online GUID Generator](https://www.guidgenerator.com/) or any other GUID generator.

Create a GUID: <https://www.guidgenerator.com/>

(If you use this site to create a GUID – You DO NOT have to run the below script – ‘$guid = ‘{‘ + (New-Guid….’)

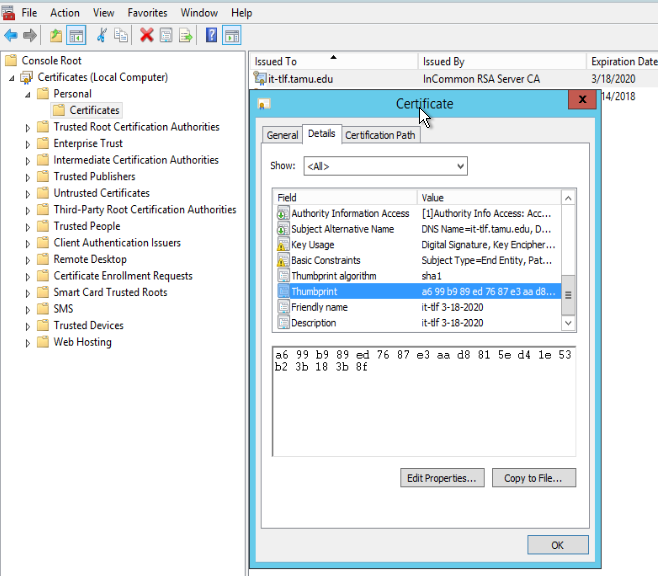
To generate a GUID in PowerShell, type:

|  |
| --- |
| $guid = '{'+ (New-Guid) + '}'  netsh http add sslcert ipport=0.0.0.0:8181 certhash=<*x*> appid=$guid |

Where <*x*> is the server certificate thumbprint.

You will need to remove the spaces, so it will look like this:

‎ a699b989ed7687e3aad8815ed41e53b23b183b8f



#### 

**STEP 6:**

#### **Forms Notification**

Create a GUID: <https://www.guidgenerator.com/>

(If you use this site to create a GUID – You DO NOT have to run the below script – ‘$guid = ‘{‘ + (New-Guid….’)

Log into the host running Forms. Open an administrative PowerShell window. Bind the SSL certificate to port 8181 by typing:

|  |
| --- |
| netsh http add sslcert ipport=0.0.0.0:8181 certhash=<*x*> appid='{<*n*>}' |

Where <*x*> is the server certificate thumbprint and <*n*> is a valid GUID.

Example:

netsh http add sslcert ipport=0.0.0.0:8181 certhash=‎a699b989ed7687e3aad8815ed41e53b23b183b8f

appid={f37d396b-fd1f-4df3-89a0-fab26f194ae7}

For more information on this topic, see the Configuring Notification Service When Using SSL section of [Laserfiche Notification Service](https://www.laserfiche.com/support/webhelp/Laserfiche/10/en-us/administration/#../Subsystems/Forms/Content/Notification-Service.htm).

**STEP 7:**

For information on how to find the certificate thumbprint, see [How to: Retrieve the Thumbprint of a Certificate](https://docs.microsoft.com/en-us/dotnet/framework/wcf/feature-details/how-to-retrieve-the-thumbprint-of-a-certificate). To find a GUID, use PowerShell, the [Online GUID Generator](https://www.guidgenerator.com/) or any other GUID generator.

Create a GUID: <https://www.guidgenerator.com/>

(If you use this site to create a GUID – You DO NOT have to run the below script – ‘$guid = ‘{‘ + (New-Guid….’)

To generate a GUID in PowerShell, type:

|  |
| --- |
| $guid = '{'+ (New-Guid) + '}'  netsh http add sslcert ipport=0.0.0.0:8181 certhash=<*x*> appid=$guid |

Where <*x*> is the server certificate thumbprint.

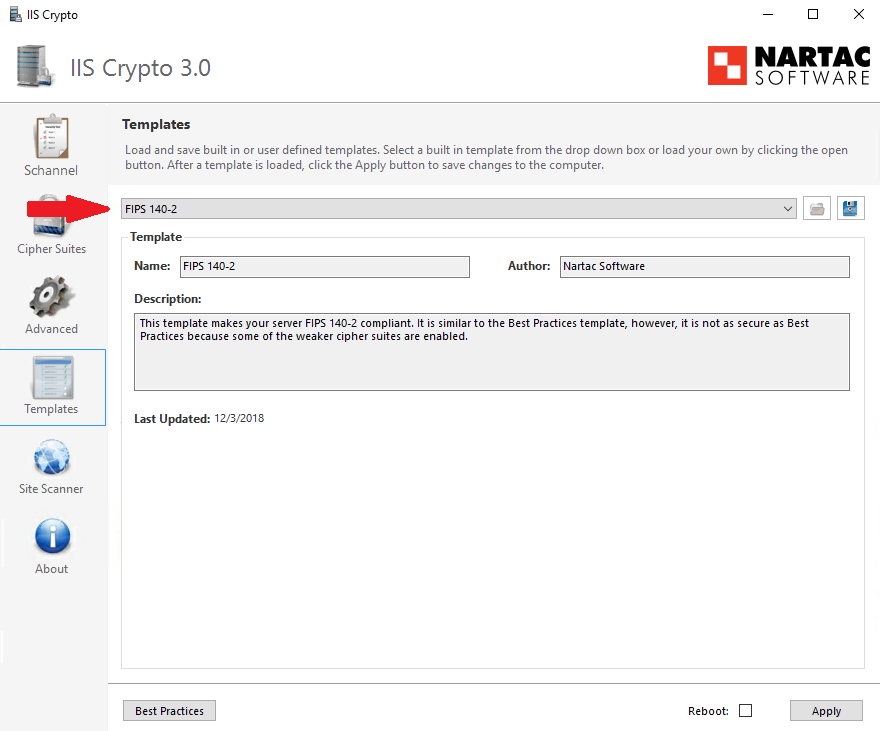
**STEP 8:**

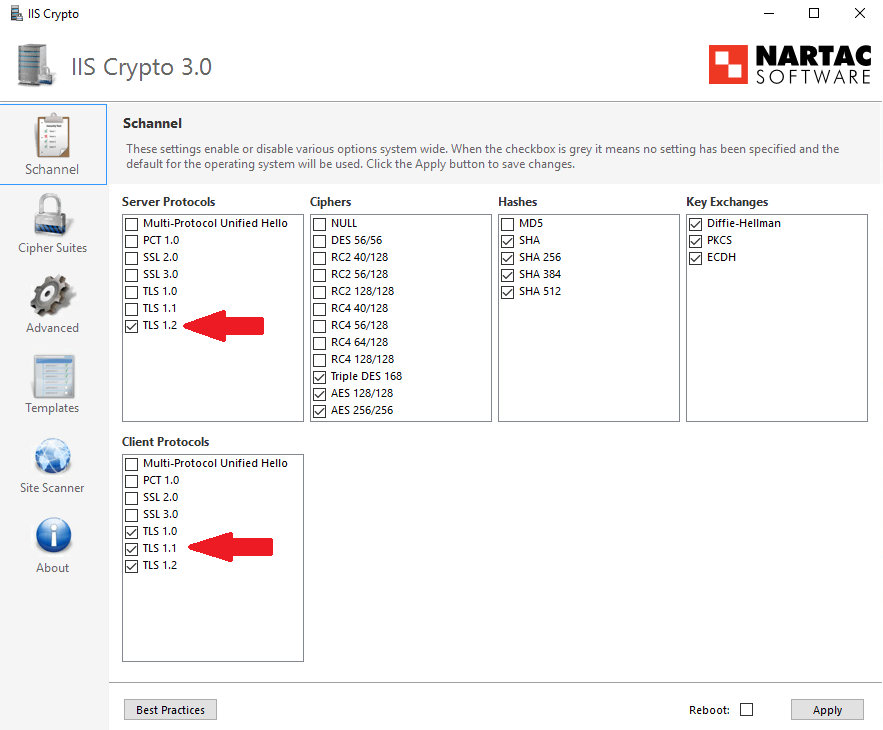
## Configuring Network Security Settings with IIS Crypto

IIS Crypto is free software developed by Nartac Software that allows administrators to easily enable or disable protocols, ciphers, hashes, and key exchange algorithms. These instructions will refer only to the GUI application.

Each server should have the following IIS Crypto configurations:

First, ensure that FIPS 140-2 is selected on the **Templates** tab.





New settings does not have TLS 1.0 or TLS 1.1 checked off.

Updated screenshot of these settings on IIS Crypto shown below.

Graphical user interface, text

Description automatically generated

Then, on the **Schannel** tab, ensure that only the **TLS 1.2** box is selected under **Server Protocols** and that **TLS 1.0, TLS 1.1, and TLS 1.2** are selected under **Client Protocols.**

!!IMPORTANT EXCEPTION!! Note: For servers that host Laserfiche Forms,

**Server Protocols** for ~~TLS 1.0 and TLS 1.1~~ TLS 1.2 should only be *enabled.* Otherwise, Forms Notification Server will not function.

If you have made any changes, select the **Reboot** box before you select **Apply.**

**STEP 9:**

### Configure Repositories and the Web Client

fqdn/Laserfiche/Configuration/ Is the below the correct url?

<https://lf.tamhsc.edu/Laserfiche/Configuration/> DO NOT have Access

Connection tab -> each repo, select SSL

Settings tab -> select SSL

Services tab -> turn on HTTPS redirection

**STEP 10: (‘Workflow Configuration Manager’ is on LFWorkflow server)**

**(Has a Red Exclamation mark under ‘Workflow Server – LEAVE ALONE?)**

Workflow configuration manager:

email servers: set SMTP

**Table

Description automatically generated**

**STEP 11: (‘Workflow Configuration Manager’ is on LFWorkflow server)**

**DO NOT know where these options are located!**

**Table

Description automatically generated**

**Has a ‘Workflow Web Services’ but DOES NOT give options listed below:**

**<http://lfworkflow.ad.tamhsc.edu/Workflow>**

**Do NOT know where these settings are located?**

**Are these below links(list) on this website?**

[**https://go.laserfiche.com/support/webhelp/workflow/9.0/en-us/content/resources/configuration/Config%20Manager/Workflow%20Web%20Service.htm#:~:text=The%20Workflow%20Web%20Service%20can,during%20the%20Laserfiche%20Workflow%20installation.&text=Open%20the%20Workflow%20Configuration%20Manager,All%20Programs%2C%20Laserfiche%2C%20Workflow**](https://go.laserfiche.com/support/webhelp/workflow/9.0/en-us/content/resources/configuration/Config%20Manager/Workflow%20Web%20Service.htm#:~:text=The%20Workflow%20Web%20Service%20can,during%20the%20Laserfiche%20Workflow%20installation.&text=Open%20the%20Workflow%20Configuration%20Manager,All%20Programs%2C%20Laserfiche%2C%20Workflow)**.**

**‘Workflow Administration Console’ connects to which server?**

**OR**

**Laserfiche Web Client 11.0 Configuration? On LFWeb server**

‘Workflow web services’

Forms config

Forms server -> SSL + HTTPS Redirect

Forms email -> SSL

Forms notification -> SSL (check IISCrypto)

Forms <-> Workflow -> SSL

**STEP 12: NO ‘Laserfiche Distributed Computing Cluster service’ on any of the Server’s Services so NO DCC Scheduler Server?**

**If they use DCC (‘Laserfiche Distributed Computing Cluster service’: LFWeb-NO, LFWorkflow-NO, LFServer-NO, LFQF-NO, LFSQL-NO)**

Perform this procedure on only the DCC Scheduler servers. To [configure the DCC Schedulers to use SSL/TLS](https://www.laserfiche.com/support/webhelp/Laserfiche/10/en-US/administration/#../Subsystems/LFAdmin/Content/DCC/DCC-SSL-TLS.htm), perform the following steps:

1. Open Windows **Services.**
2. Stop the **Laserfiche Distributed Computing Cluster service** if it is running.
3. Open **C:\ProgramData\Laserfiche\Distributed Computing Cluster\Config\SchedulerConfig.xml** in an XML or text editor.
4. Under the <SchedulerConfigFile> element, paste the following XML.

**Note**: The XML is space- and case-sensitive.

<TaskModuleConfiguration>

<TaskConfiguration>

<TaskName>OCR.Image Cleanup</TaskName>

<Settings>ForceSSL=yes</Settings>

</TaskConfiguration>

<TaskConfiguration>

<TaskName>OCR.OCR</TaskName>

<Settings>ForceSSL=yes</Settings>

</TaskConfiguration>

<TaskConfiguration>

<TaskName>OCR.Task Creator</TaskName>

<Settings>ForceSSL=yes</Settings>

</TaskConfiguration>

</TaskModuleConfiguration>

1. Save the changes.
2. In Windows Services, restart the **Laserfiche Distributed Computing Cluster service.**

might have to take apart and rebuild cluster

Audit Trail

Repo:

Use the following settings for the repository connection:

|  |  |
| --- | --- |
| **Option** | **Value** |
| User | Audit Trail |
| Password | $Audit Trail password |
| Win Auth | false / off |
| SSL | true / on |

The Audit Trail user must have the “Retrieve Audit Data” feature right within the repository.

Find version of .NETFrame:

CMD:

***reg query "HKLM\SOFTWARE\Microsoft\Net Framework Setup\NDP" /s***