FlexNet Manager Suite

Configuring Transport Layer Security (TLS) Protocols

February 2018, Version 1.0

Introduction

FlexNet Manager Suite requires Microsoft Transport Layer Security (TLS) protocols to upload and download from the FlexNet inventory beacons. FlexNet Manager Suite supports TLS versions 1.0 - 1.2

This purpose of this document is to describe the configuration changes required if you wish to force the use of TLS v1.1 or v1.2

Only FlexNet Beacon versions 2017 R1 or newer supports TLS 1.1 and TLS 1.2 protocols. Please upgrade your FlexNet inventory beacon if it is running an older version.

This table gives an understanding of what protocols are supported on these Windows Operating Systems:

	TLS 1.0	TLS 1.1	TLS 1.2
Windows XP & Windows Server 2003	✓	X	X
Windows Vista & Windows Server 2008	✓	✓	✓
Windows 7 & Windows Server 2008 R2	✓	✓	✓
Windows 8 & Windows Server 2012	✓	✓	✓
Windows 8.1 & Windows Server 2012 R2	✓	✓	✓
Windows 10 & Windows Server 2016	✓	✓	✓

Note: TLS 1.1 & TLS 1.2 are enabled by default on post Windows 8.1 releases. Prior to this they were disabled by default. Administrators for the older versions will have to enable the settings via the registry.

Configuration and Installation of .NET

Your chosen configuration will depend on the version of .NET that is installed, or that you wish to install.

Configuration with .NET v4.6.2

1. Install .NET v4.6.2

This is the recommended option. Microsoft .NET Framework 4.6.2 or higher (Web/Offline) can be used with Microsoft operating systems:

- Windows 7 SP1
- Windows 8.1
- Windows Server 2008 R2 SP1
- Windows Server 2012
- Windows Server 2012 R2

The .NET v4.6.2 web installer will automatically determine the components applicable for each particular platform. The online version is It is available from:

https://www.microsoft.com/en-us/download/details.aspx?id=53345

The offline version can be downloaded from here:

https://www.microsoft.com/en-au/download/details.aspx?id=53344

2. Configure your FlexNet Beacon

To enable the TLS protocols, you will need to add new registry entries

For that, please follow these steps:

1. Start the registry editor by clicking on **Start** and **Run**. Type in `regedit` into the Run field.
2. As you will be editing the registry, that may have detrimental effects on your computer if done incorrectly, it is strongly advised to make a backup. To do this, highlight **Computer** at the top of the registry tree. Now backup the registry by clicking on **File** and then on **Export**. Select a file location to save the registry file.
3. Browse to the following registry key:

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
   ```

4. Right click on the **Protocols** folder and select **New** and then **Key** from the drop-down menu. This will create new folder. Rename this folder to **TLS 1.1** or **TLS 1.2** - depending on the protocol you want to enable.

5. Right click on the **TLS 1.1** or **TLS 1.2** key and add two new key underneath it.
6. Rename the new keys as:
    - Client
    - Server
7. Right click on the **Client** key and select **New** and then **DWORD (32-bit) Value** from the drop-down list.
8. Rename the **DWORD** to **DisabledByDefault**.
9. Right-click the name **DisabledByDefault** and select **Modify...** from the drop-down menu.
10. Ensure that the **Value** data field is set to **0** and the **Base** is **Hexadecimal**. Click on **OK**.
11. Create another **DWORD** for the **Client** key as you did in **Step 7**.
12. Rename this second **DWORD** to **Enabled**.
13. Right-click the name **Enabled** and select **Modify...** from the drop-down menu.
14. Ensure that the Value data field is set to **1** and the **Base** is **Hexadecimal**. Click on **OK**.
15. Repeat steps **7** to **14** for the **Server** key (by creating two DWORDs, **DisabledByDefault** and **Enabled**, and their values underneath the **Server** key).
16. Reboot your server

After the reboot, the server will be able to communicate through the TLS 1.1 or TLS 1.2 protocol you enabled.

Additional Steps Required to Enable TLS 1.1 or TLS 1.2 on **Windows Server 2016**

1. Start the registry editor by clicking on **Start** and **Run**. Type in `regedit` into the Run field.
2. As you will be editing the registry, that may have detrimental effects on your computer if done incorrectly, it is strongly advised to make a backup. To do this, highlight **Computer** at the top of the registry tree. Now backup the registry by clicking on **File** and then on **Export**. Select a file location to save the registry file.
3. Browse to the following registry key:

    `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NetFramework\v4.0.30319`
4. Right-click on the right pane and create a new DWORD (32-bit) Value with Name **SchUseStrongCrypto**.
5. Ensure that the **Value** data field is set to **1** and the **Base** is **Hexadecimal**. Click on **OK**.
6. Repeat steps 4 and 5 for the registry key:

    `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NetFramework\v4.0.30319`
7. Reboot the server

Configuration with .NET v4.5.x

If you need to restrict your version of .NET to 4.5.x add the following registry entries.

Configure your FlexNet Beacon

1. Start the registry editor by clicking on **Start** and **Run**. Type in `regedit` into the Run field.
2. As you will be editing the registry, that may have detrimental effects on your computer if done incorrectly, it is strongly advised to make a backup. To do this, highlight **Computer** at the top of the registry tree. Now backup the registry by clicking on **File** and then on **Export**. Select a file location to save the registry file.
3. Browse to the following registry key:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols`
4. Right click on the **Protocols** folder and select **New** and then **Key** from the drop-down menu. This will create new folder. Rename this folder to **TLS 1.1** or **TLS 1.2** - depending on the protocol you want to enable.
5. Right click on the **TLS 1.1** or **TLS 1.2** key and add two new key underneath it.
6. Rename the new keys as:
   - Client
   - Server
7. Right click on the **Client** key and select **New** and then **DWORD (32-bit) Value** from the drop-down list.
8. Rename the **DWORD** to **DisabledByDefault**.
9. Right-click the name **DisabledByDefault** and select **Modify...** from the drop-down menu.
10. Ensure that the **Value** data field is set to **0** and the **Base** is **Hexadecimal**. Click on **OK**.
11. Create another **DWORD** for the **Client** key as you did in **Step 7**.
12. Rename this second **DWORD** to **Enabled**.
13. Right-click the name **Enabled** and select **Modify...** from the drop-down menu.
14. Ensure that the **Value** data field is set to 1 and the Base is Hexadecimal. Click on OK.
15. Repeat steps 7 to 14 for the **Server** key (by creating two DWORDs, **DisabledByDefault** and **Enabled**, and their values underneath the **Server** key).
16. Reboot your server.

After the reboot, the server will be able to communicate through the TLS 1.1 or TLS 1.2 protocol you enabled.

Additional Steps Required to Enable TLS 1.1 or TLS 1.2 on **Windows Server 2016**

1. Start the registry editor by clicking on **Start** and **Run**. Type in `regedit` into the Run field.
2. As you will be editing the registry, that may have detrimental effects on your computer if done incorrectly, it is strongly advised to make a backup. To do this, highlight **Computer** at the top of the registry tree. Now backup the registry by clicking on **File** and then on **Export**. Select a file location to save the registry file.
3. Browse to the following registry key:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NetFramework\v4.0.30319`
4. Right-click on the right pane and create a new DWORD (32-bit) Value with Name **SchUseStrongCrypto**.
5. Ensure that the **Value** data field is set to **1** and the **Base** is **Hexadecimal**. Click on OK.
6. Repeat steps 4 and 5 for the registry key:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NetFramework\v4.0.30319`
7. Reboot the server

Enabling browser support for TLS 1.1 and TLS 1.2

FlexNet Manager Suite supports TLS 1.0, TLS 1.1 and TLS 1.2. Though some browser versions support TLS 1.1 and TLS 1.2 by default others require the TLS version to be configured.

The following browsers support TLS 1.1 and 1.2:

- Chrome - v30 supports TLS 1.2. Previous to this only up to TLS 1.1 was supported
- Firefox - v27 enables TLS 1.1 and 1.2 by default.
- Internet Explorer - v11 supports TLS 1.2 from Feb 2013.
- Safari - v5 on iOS and v7 on OS X have added support for up to TLS 1.2.

Browsers may require configuration to support TLS 1.1 and TLS 1.2. This configuration can be achieved through the steps provided below.

Note: Please refer to the Release Notes for the latest information relating to browser support for FlexNet Manager Suite.

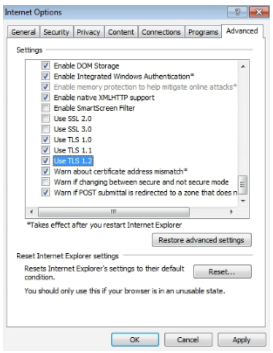
Firefox

Firefox - v27 enables TLS 1.1 and 1.2 by default. FlexNet Manager only supports Firefox – v 45 or higher. No configuration change required for Firefox.

Internet Explorer

To change setting for Internet Explorer versions 10 & 11:

- Go to Tools and select **Internet Options**
- Select the **Advanced** tab in Internet Options
- Enable(check) TLS 1.1, TLS 1.2 and also disable (uncheck) SSL 3.0 for additional security
- Click on **Apply** and **OK** to complete the procedure

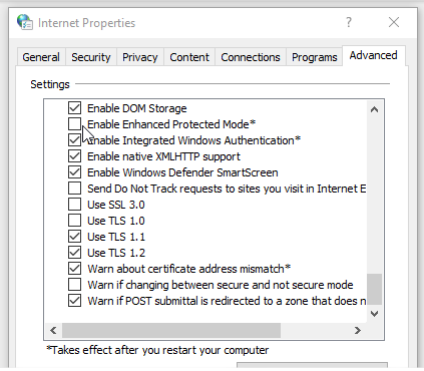


Chrome

All versions of Google Chrome above version 38 are compatible by default, however FlexNet Manager Suite only supports Chrome – v46 or higher.

To change setting for Chrome:

- Open the browser.
- Select **Settings** from the menu.
- Scroll down and select A**dvanced** settings.
- Scroll down to system section and click on **Open proxy settings**.
- Choose the Advanced tab and scroll to the Security section.
- Check Use TLS 1.1 or Use TLS 1.2.
- Press OK.



Safari

Desktop Safari versions 7 and higher for OS X 10.9 (Mavericks) and higher are, compatible with TLS 1.1 and higher, by default. Note thatFlexNet Manager Suite only supports Safari – v7 or higher.

Other Resources and Links

More Information

Item	Description
Flexera Software website	Information about Flexera Software http://www.flexerasoftware.com
Support	Support website, including the knowledge base https://flexeracommunity.force.com/customer
Product downloads	Flexera Software Product and License Center https://flexera.flexnetoperations.com/flexnet/operationsportal/startPage.do
Email sign-up for product announcements	For notification of FlexNet Manager Suite software updates, including hot fixes http://learn.flexerasoftware.com/SLO-FMS-Software-Content-Library-Updates