How to Configure Microsoft Windows 7 to use TLS Version 1.2

Overview

This document explains how to configure your Microsoft Windows® 7 workstation and Microsoft Outlook® 2010 email clients to use Transport Layer Security (TLS) protocol version 1.2.

Important:

- As of cPanel & WHM version 68, we **only** support Transport Layer Security (TLS) protocol version 1.2, and we enable TLSv1.2 by default.
  - We will **only** support applications that use TLSv1.2 and **strongly** recommend that you enable TLSv1.2 on your server.
- The instructions in this document **only** pertain to servers that run the Windows 7 operating system.
- We **strongly** recommend that you do **not** adjust the cipher and protocol settings for the Exim and Dovecot services on Windows 7. Servers on this operating system fail PCI compliance scans because of unpatched security vulnerabilities that exist in the following email clients:
  - Outlook 2007.
  - Outlook 2010.

Create registry keys

Install Windows update

You **must** download and install the `KB3140245` Windows update from the Microsoft Update Catalog. This update will create the registry key paths in which you will create new registry keys. These registry keys will allow you to enable TLSv1.2 on your server.

After you download and install the update, you **must** restart your computer for the changes to take effect.

Add a registry key for Windows HTTP services

To add a registry key for Windows HTTP services, perform the following steps:

1. From the Windows *Start* menu, enter *regedit.exe* in the *Search* text box.
2. Click *regedit.exe* to open the *Registry Editor.*
3. Navigate to the following registry path:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
```

4. Select the `WinHttp` key.

5. From the *Menu* bar, click *Edit*, select *New*, and click *DWORD (32-bit) Value*.

   > **Note:**
   >
   > On 64-bit systems, click *QWORD (64-bit) Value*.

6. Enter `DefaultSecureProtocols` as the DWORD value's name.
7. Right-click the file and select *Modify* from the *Context* menu.
8. Enter `A00` in the *Value Data* text box and click *OK*.

> **Important:**
>
> If your workstation runs on a 64-bit system, you **must also** perform steps 5-8 for the following key:
>
> ```
> HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp
> ```

Add a registry key for the TLS directories

To add registry keys for TLS versions 1.1 and 1.2, perform the following steps:

1. Navigate to the following registry path:

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1
   ```

2. Select the `Client` key.
3. From the *Menu* bar, click *Edit*, select *New*, and click *DWORD (32-bit) Value*.

   > **Reminder:**
   >
   > On 64-bit systems, click *QWORD (64-bit) Value*.

4. Enter `DisabledByDefault` as the DWORD value's name.
5. Right-click the file and select *Modify* from the *Context* menu.
6. Enter `0` in the *Value Data* text box and click *OK*.
7. Navigate to the `TLS1.2` registry path and open the `Client` key.
8. Repeat steps 2-6 and click *OK.*

Apply the settings.

After you modify your registry keys, you **must** restart your workstation to apply the registry settings. When your workstation restarts, create a test email account in Microsoft Outlook and configure the following settings in the *Advanced* section of Microsoft Outlook's *Internet E-Mail Settings* interface:

- Enter `993` in the *Incoming Server (IMAP)* text box or `995` in the *Incoming Server (POP3)* text box.
- Enter `465` in the *Outgoing Server (SMTP)* text box.

After you finish, click *OK*. Your Microsoft Outlook account will now successfully connect to your cPanel server's mail services.

Installation scripts

We created two scripts that will automatically perform the actions that this document describes. To use these scrtps, perform the following steps:

1. Open the Windows *PowerShell* application.
2. Navigate to the directory of you choice.
3. Create the `install-kb.ps1` and `tls-reg-edit.ps1` files.
4. Open the `install-kb.ps1` file with a text editor and add the following information:

> **Note:**
>
> This script downloads and installs the KB3140245 Windows update.

```
Import-Module BitsTransfer

$arch=(Get-WmiObject -Class Win32_operatingsystem).Osarchitecture

If ($arch -eq "32-bit") {
    $kbUrl32 = "http://download.windowsupdate.com/c/msdownload/update/software/updt/2016/04/windows6.
1-kb3140245-x86_cdafb409afbe28db07e2254f40047774a0654f18.msu"
    $kb32 = "windows6.1-kb3140245-x86_cdafb409afbe28db07e2254f40047774a0654f18.msu"
    Start-BitsTransfer -source $kbUrl32
    wusa $kb32 /log:install.log
}
Else {
    $kbUrl64 = "http://download.windowsupdate.com/c/msdownload/update/software/updt/2016/04/windows6.
1-kb3140245-x64_5b067ffb69a94a6e5f9da89ce88c658e52a0dec0.msu"
    $kb64 = "windows6.1-kb3140245-x64_5b067ffb69a94a6e5f9da89ce88c658e52a0dec0.msu"
    Start-BitsTransfer -source $kbUrl64
    wusa $kb64 /log:install.log
}
```

5. Open the `tls-reg-edit.ps1` file with a text editor and add the following information:

> **Note:**
>
> This script creates registry keys in the following files:
>
> ```
> HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp
> HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet
> Settings\WinHttp
> HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
> 1.1
> HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
> 1.2
> ```

```
$arch=(Get-WmiObject -Class Win32_operatingsystem).Osarchitecture
$reg32bWinHttp = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp"
$reg64bWinHttp = "HKLM:\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet
Settings\WinHttp"
$regWinHttpDefault = "DefaultSecureProtocols"
$regWinHttpValue = "0x00000a00"
$regTLS11 = "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1
\Client"
$regTLS12 = "HKLM:SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2
\Client"
$regTLSDefault = "DisabledByDefault"
$regTLSValue = "0x00000000"

Clear-Host
Write-Output "Creating Registry Keys...`n"
Write-Output "Creating registry key $reg32bWinHttp\$regWinHttpDefault with value $regWinHttpValue"

IF(!(Test-Path $reg32bWinHttp)) {
    New-Item -Path $reg32bWinHttp -Force | Out-Null
    New-ItemProperty -Path $reg32bWinHttp -Name $regWinHttpDefault -Value $regWinHttpValue -
PropertyType DWORD -Force | Out-Null
}
ELSE {
    New-ItemProperty -Path $reg32bWinHttp -Name $regWinHttpDefault -Value $regWinHttpValue -
PropertyType DWORD -Force | Out-Null
}

IF($arch -eq "64-bit") {
    Write-Output "Creating registry key $reg64bWinHttp\$regWinHttpDefault with value $regWinHttpValue"
    IF(!(Test-Path $reg64bWinHttp)) {
        New-Item -Path $reg64bWinHttp -Force | Out-Null
        New-ItemProperty -Path $reg64bWinHttp -Name $regWinHttpDefault -Value $regWinHttpValue -
PropertyType DWORD -Force | Out-Null
    }
    ELSE {
        New-ItemProperty -Path $reg64bWinHttp -Name $regWinHttpDefault -Value $regWinHttpValue -
PropertyType DWORD -Force | Out-Null
    }
}

Write-Output "Creating registry key $regTLS11\$regTLSDefault with value $regTLSValue"

IF(!(Test-Path $regTLS11)) {
    New-Item -Path $regTLS11 -Force | Out-Null
    New-ItemProperty -Path $regTLS11 -Name $regTLSDefault -Value $regTLSValue -PropertyType DWORD -
Force | Out-Null
    }
ELSE {
    New-ItemProperty -Path $regTLS11 -Name $regTLSDefault -Value $regTLSValue -PropertyType DWORD -
Force | Out-Null
}

Write-Output "Creating registry key $regTLS12\$regTLSDefault with value $regTLSValue"

IF(!(Test-Path $regTLS12)) {
    New-Item -Path $regTLS12 -Force | Out-Null
    New-ItemProperty -Path $regTLS12 -Name $regTLSDefault -Value $regTLSValue -PropertyType DWORD -
Force | Out-Null
    }
ELSE {
    New-ItemProperty -Path $regTLS12 -Name $regTLSDefault -Value $regTLSValue -PropertyType DWORD -
Force | Out-Null
}

Write-Output "`nComplete!"
```

6. Run the scripts from the directory in which you saved the files, for example:

```
Set-ExecutionPolicy Bypass -Scope Process ; .\install-kb.ps1
Set-ExecutionPolicy Bypass -Scope Process ; .\tls-reg-edit.ps1
```

7. Restart your workstation for the changes to take effect.

Additional documentation

Content by label

There is no content with the specified labels